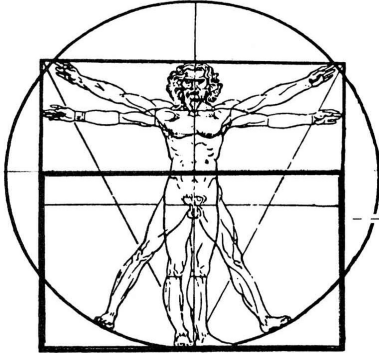


Mathematics

Office: Ground Floor
163 Ditchling Rise
Brighton BN1 4QR
UK



Monday 21st December 2009

by: Jim Adams

Version M 4.4A

EXPONENTIATION (Second Edition)

© 2008, 2009 Jim Adams

Exponentiation

JIM ADAMS

<http://www.jimhadams.com>

Original Version M 2.2. 6th February 2008.
Version M 2.5. 29th February 2008. (Section 7).
Version M 2.8. 28th April 2008. (Sections 8 & 9).
Version M 2.9. 27th May 2008.
Version M 3.1. 14th July 2008. (Extended Sections 5 & 8).
Version M 3.4. 15th August 2008. (First Edition complete).

NOTE: Sections 9 on ramification and complex exponentiation and 11 on intricate representations of $\text{Mat}(2^n, \mathbf{R})$ were removed from Version M 3.4, with the intention that these topics would reappear in future versions.

Version M 3.6. 21st December 2008. (Extended Section 8).
Version M 3.7. 25th January 2009. (Extended Section 12).
Version M 3.8. 15th June 2009. (Extended Sections 1 & 5, reorganisation incorporating Section 6 and a reinsert of part of Section 11).
Version M 4.2A. 5th October 2009. (Section 1 reduced, Sections 9 – 14 removed, Section reorganisations)

1.1 Introduction.

In this outline of our conceptual work, a review largely based on elementary methods, which have been common mathematical currency for over two centuries, we describe explorations of the mathematical landscape concerning global field theorems for exponential powers.

In Section 1.2, we introduce an exponential notation.

Section 2.1 restates foundational rules for real exponentiation, providing proofs for the basic '*binomial exponent*' and '*geometric exponent*' theorems.

Section 2.2 continues with new cyclotomic variants of the '*Fermat subtraction*', '*Fermat addition*' and '*linear combination*' factorisation theorems, the latter being a formula that is a linear combination of the previous two.

Section 2.3 develops in many variables the linear combination factorisation theorem.

Prime number, factorisation and divisibility theorems are discussed in Section 3. In particular, we obtain primality conditions not dealt with in most textbooks, e.g. for ‘*generalised Fermat*’ numbers, for positive natural numbers γ or $\delta > 1$ and p , we prove that no number of the form $\gamma^p + \delta^p$ is prime, except for the possibilities $p = 1$ or p a power of 2. For ‘*generalised Mersenne*’ numbers, no representations of primes are of the form $\gamma^p - \delta^p$, except for the possibilities $p = 1$, or $\delta = (\gamma - 1)$ and p prime. We also discuss a linear combination of powers prime number theorem and continue with a discussion on factorisation of p th powers $\gamma^p \pm \delta^p$.

This Section also discusses developments of *Fermat’s little theorem*, including theorems connected with *reciprocity*.

Section 4 analyses using elliptic curves the number of solutions mod 4 of differences and sums of p th and different powers.

I would like to thank especially Doly García for discussions and Roger Goodwin for his advice, and to thank the mathematics department of the University of Sussex in providing facilities for checking some long computations on Quadronacci numbers.

1.2 The $a^b = a \uparrow b$ Ackermann-Knuth notation for exponentiation. [4]

We use sparingly a special symbolism to obtain our results and think a supplementary notation “ \uparrow ” for $a \uparrow b = a^b$ is suggestive and appropriate. “ $a \uparrow b$ ” must coexist with the current convention, so we would still use e.g. $\sin^2 \theta$. This has the advantages of being more compact than $\exp\{b\}$, complicated expressions become more visible and simpler to notate, long sequences of exponents of exponents become easy to write and friendly on line spacing, the choice between $(a \uparrow b) \uparrow c$ and $a \uparrow (bc)$ allows flexibility and nuance, and because usually $a \uparrow (b \uparrow c) \neq (a \uparrow b) \uparrow c$, the non-associative nature of exponentiation becomes easy to specify.

2.1 Fundamental exponential theorems for real numbers.

Let a, b, \dots to $h, \alpha, \beta, \gamma, \delta \in \mathbf{R}^+$ be non-negative real numbers and j, k, \dots to $z \in \mathbf{N}$ be natural numbers. \mathbf{N} starts from 1, unless 0 is otherwise indicated. Multiplication will take precedence over exponentiation in implicit bracketing. We admit $\pm[(-a) \uparrow (\pm p)]$ and $\pm[a \uparrow (\pm b)]$ as terms, but not otherwise $\pm[(-a) \uparrow (\pm b)]$.

Factorisation of real numbers, or of complex numbers $a + ib$, is not unique. Natural numbers factorise uniquely, and there is a type of unique factorisation for Heegner numbers, given by $p + q\sqrt{-1}$, $p + q\sqrt{-2}$ or $\frac{1}{2}(p + q\sqrt{-r})$, where $-r$ is one of $-3, -7, -11, -19, -43, -67$ or -163 .

Since exponentiation is in general not associative, we need to understand both sides of $(a \uparrow b) \uparrow c \neq a \uparrow (b \uparrow c)$, which is one of the principal objectives of our paper. Now $(a \uparrow b) \uparrow c = a \uparrow (b \times c)$, $(a \times b) \uparrow c = (a \uparrow c) \times (b \uparrow c)$, $a \uparrow (b + c) = (a \uparrow b) \times (a \uparrow c)$ and the binomial theorem is $(a + b) \uparrow q = \sum_{r=0}^q [q!/r!(q-r)!] a^r b^{q-r}$. We adopt the convention that $0! = 1$ and writing linearly put $a \times q = \sum_{r=0}^q a$, where the sum is 0 if $q = 0$, and $a \uparrow q = \prod_{r=0}^q a$, where the product is 1 if $q = 0$.

Of course, $a \uparrow (b \uparrow c)$ may be resolved immediately using the formula

$$a \uparrow (b \uparrow (c + d)) = a \uparrow [(b \uparrow c)(b \uparrow d)],$$

or equivalently

$$\begin{aligned} a \uparrow (b \uparrow c) &= a \uparrow \{d[b \uparrow (c - \log_b d)]\} \\ &= \{a \uparrow [b \uparrow (c - \log_b d)]\} \uparrow d. \blacksquare \end{aligned}$$

In comparison with the rule for a^q in terms of *products* above, the binomial theorem for $(1 + m)^q$ gives an inductive formula for p^q , $p > 2$, in terms of *sums*.

$$p^q = q! \{ \Sigma(t = 0, p - 3) [\Sigma(r_{p-2-t} = 0, q - \Sigma(u = 0, t - 1)r_{p-2-u})(1/r_{p-2-t}!) [\Sigma(r_0 = 0, q - \Sigma(v = 0, t)r_{p-2-v})(1/r_0! [q - \Sigma(w = 0, t + 1)r_{p-2-w}!])]] \}.$$

Proof. We employ a proof by induction. Using a new variable s , which starts from the first term $s = 0$, the $(s + 1)$ th term in a binomial expansion of $(1 + p)^q$ is

$$[q!/s!(q - s)!][p \uparrow (q - s)].$$

Hence, putting $s = r_{p-1}$, the sum of all these terms is

$$A_{1+p,q} = q! \{ \Sigma(r_{p-1} = 0, q)(1/r_{p-1}!) [1/(q - r_{p-1})!] [p \uparrow (q - r_{p-1})] \},$$

so since the binomial theorem gives

$$2 \uparrow (q - r_1) = (1 + 1) \uparrow (q - r_1) = \Sigma(r_0 = 0, q - r_1) \{ (q - r_1)! / [r_0!(q - r_1 - r_0)!] \},$$

the binomial expansion, $A_{1+p,q}$, for $(1 + p) \uparrow q$, $p = 2$, is equal to our postulated formula

$$3 \uparrow q = q! [\Sigma(r_1 = 0, q)(1/r_1!) \{ \Sigma(r_0 = 0, q - r_1) [1/r_0!(q - r_1 - r_0)!] \}].$$

Now, assuming the formula for $p \uparrow r$, with $r = q - r_{p-1} \leq q$, above

$$\begin{aligned} A_{1+p,q} &= q! \{ \Sigma(r_{p-1} = 0, q)(1/r_{p-1}!) [1/(q - r_{p-1})!] \{ (q - r_{p-1})! \Sigma(t = 0, p - 3) \\ &\quad [\Sigma(r_{p-2-t} = 0, q - \Sigma(u = 0, t)r_{p-1-u})(1/r_{p-2-t}!) \\ &\quad [\Sigma(r_0 = 0, q - \Sigma(v = 0, t + 1)r_{p-1-v})(1/r_0!(q - \Sigma(w = 0, t + 2)r_{p-1-w}!))] \} \} \}. \end{aligned}$$

Rearranging where t varies from 0 to $p - 3$, and cancelling terms

$$\begin{aligned} A_{1+p,q} &= q! \{ \Sigma(t = 0, p - 3) [\Sigma(r_{p-1} = 0, q)(1/r_{p-1}!) \\ &\quad [\Sigma(r_{p-2-t} = 0, q - \Sigma(u = 0, t)r_{p-1-u})(1/r_{p-2-t}!) \\ &\quad [\Sigma(r_0 = 0, q - \Sigma(v = 0, t + 1)r_{p-1-v})(1/r_0!(q - \Sigma(w = 0, t + 2)r_{p-1-w}!))] \} \} \}, \end{aligned}$$

so the second line summation starts from r_{p-2} . This implies

$$\begin{aligned} A_{1+p,q} &= q! \{ \Sigma(t = 0, p - 2) [\Sigma(r_{p-1-t} = 0, q - \Sigma(u = 0, t - 1)r_{p-1-u})(1/r_{p-1-t}!) \\ &\quad [\Sigma(r_0 = 0, q - \Sigma(v = 0, t)r_{p-1-v})(1/r_0!(q - \Sigma(w = 0, t + 1)r_{p-1-w}!))] \} \}, \end{aligned}$$

where t varies from 0, then 1 (e.g. r_{p-2} sum) to $p - 2$, that is, $A_{1+p,q} = (1 + p) \uparrow q$. \blacksquare

Using $a \uparrow (\Sigma(j = 0, k) z_j) = \Pi(j = 0, k)(a \uparrow z_j)$, $a \uparrow (p \uparrow q)$ can be expanded out using the above formula to give the *binomial exponent factorisation theorem (BEFT)*, or expanded out fully as $n \uparrow (p \uparrow q)$.

The *geometric exponent factorisation theorem (GEFT)* for $a \uparrow (b^{cq})$ is

$$a \uparrow (b^{cq}) = a \{ \Pi(r = 0, q - 1) a \uparrow [(b^c - 1)b^{cr}] \}.$$

Proof. Consider the geometric series

$$S_n = \alpha + \alpha b^c + \alpha b^{2c} + \dots + \alpha b^{nc}.$$

The sum is

$$S_n = \alpha [1 - b^{c(n+1)}] / [1 - b^c].$$

Insert $\alpha = [b^c - 1]$ and $n = q - 1$. Then the sum becomes

$$[b^{cq} - 1] = [b^c - 1] \{ (b^c) \uparrow 0 + (b^c) \uparrow 1 + \dots + (b^c) \uparrow (q - 1) \},$$

yielding

$$a \uparrow [b^{cq} - 1] = \Pi(r = 0, q - 1) a \uparrow \{ [b^c - 1] [b^c \uparrow r] \}. \blacksquare$$

The geometric series is related to *cyclotomic equations*, studied in the generalised Fermat factorisation theorems of section 2.2.

Incidentally, when the *arithmetic* (a special case of *Bernoulli*) series formula

$$a^{q(q+1)} = [\prod_{r=0}^q a^{2r}]$$

is combined with the *GEFT* above, it gives the result

$$a^q = (a^{1/2})^{\{ \prod_{r=0}^q a^{\uparrow[(4r - 3/2(q+1))/(2q+3)]} \}},$$

which reduces to

$$q = 1/2 + \Sigma(r=0, q)[(4r - 3/2(q+1))/(2q+3)],$$

as can be reconfirmed by routine calculation. A permutation of the argument gives

$$q = -3/2 + \Sigma(r=0, q)[(4r - 3/2(q+1))/(2q-1)].$$

Proof. We give a proof motivated by exponentiation. The arithmetic series sum is

$$\Sigma(r=0, q) r = q(q+1)/2,$$

thus

$$a^{q(q+1)} = [\prod_{r=0}^q a^{r}]^2.$$

Now

$$q(q+1) = (q + 1/2)^2 - 1/4.$$

It follows that

$$a^{\uparrow(q + 1/2)^2} = a^{1/4} [\prod_{r=0}^q a^{2r}].$$

Applying the geometric formula gives

$$\begin{aligned} a^{\uparrow(q + 1/2)^2} &= a^{\{ \prod_{r=0}^q a^{\uparrow[(q - 1/2)((q + 1/2)\uparrow r]} \}} \\ &= a[a^{\uparrow(q - 1/2)}][a^{\uparrow[(q - 1/2)(q + 1/2)}] \\ &= a[a^{\uparrow(q - 1/2)}]^{\uparrow(q + 3/2)}. \end{aligned}$$

We deduce

$$[a^{\uparrow(q - 1/2)}]^{(q + 3/2)} = a^{-3/4} [\prod_{r=0}^q a^{2r}],$$

the last product having $q + 1$ factors, from $r = 0$ to $r = q$. This right hand side is

$$[a^{-3(q+1)/4(q+1)}][\prod_{r=0}^q a^{2r}] = \prod_{r=0}^q a^{(2r - 3/4(q+1))}.$$

Thus exponentiating by $1/(q + 3/2)$

$$[a^{(q - 1/2)}] = \prod_{r=0}^q [a^{\uparrow(2r - 3/4(q+1))}]^{2/(2q+3)},$$

giving

$$a^q = a^{1/2} \prod_{r=0}^q [a^{\uparrow(4r - 3/2(q+1))}]^{1/(2q+3)}.$$

If instead we interchange $(q - 1/2)$ and $(q + 3/2)$ and exponentiate by $1/(q - 1/2)$

$$a^q = a^{-3/2} \prod_{r=0}^q [a^{\uparrow(4r - 3/2(q+1))}]^{1/(2q-1)}. \blacksquare$$

2.2 Generalised cyclotomic Fermat factorisation theorems.

The q th *Fermat number* is $F_q = 2^{\uparrow(2\uparrow q)} + 1$. So $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ and $F_5 = 4294967297$. Our theorems relate to generalised such F_q . As Fermat knew, the extended Mersenne number $F_q - 2 = \prod_{r=0}^{q-1} F_r$. The *second Fermat subtraction factorisation theorem* example contains this result for $a, p = 2$ and $f = 1$.

An example of the *first Fermat subtraction factorisation theorem (first FSFT)* is

$$a^{\uparrow(p^c)} = \{ [a^{\uparrow(p^{c-1})} - 1][\Sigma(s=0, p-1)[(a^{\uparrow(p^{c-1})})^{\uparrow s}]] \} + 1.$$

The *first FSFT* is

$$\begin{aligned} a^{\uparrow[(bp)^c]} - f^{\uparrow[(gp)^h]} &= \\ & \{ [a^{\uparrow((bp)^{c-1})}]^b - [f^{\uparrow((gp)^{h-1})}]^g \} \{ \Sigma(s=0, p-1) \\ & [(a^{\uparrow[(bp)^{c-1}])^{\uparrow bs}}][f^{\uparrow[(gp)^{h-1}])^{\uparrow g(p-1-s)}] \}. \end{aligned}$$

Proof. Introducing $\alpha = \gamma^p$ and $\beta = \delta^p$, we explore the *cyclotomic* formula

$$\gamma^p - \delta^p = (\gamma - \delta)(\gamma^{p-1} + \gamma^{p-2}\delta + \gamma^{p-3}\delta^2 + \dots + \delta^{p-1}),$$

which can be written in the form

$$\alpha - \beta = [\alpha^{1/p} - \beta^{1/p}]\{\Sigma(s = 0, p - 1)[\alpha^{s/p}][\beta^{1-1/p-s/p}]\}.$$

We obtain our result using

$$\alpha = a \uparrow [(bp)^c] = a \uparrow [(bp)^1 (bp)^{c-1}] = (a \uparrow [(bp)^{c-1}]) \uparrow bp$$

and similarly

$$\beta = f \uparrow [(gp)^h] = (f \uparrow [(gp)^{h-1}]) \uparrow gp. \blacksquare$$

An example of the *second FSFT* is

$$a \uparrow (p^q) - f \uparrow (p^q) = [a - f] \Pi(r = 0, q - 1) \{\Sigma(s = 0, p - 1)[a \uparrow (s(p^{q-1-r}))][f \uparrow ((p - 1 - s)(p^{q-1-r}))]\}.$$

The *second FSFT* for free parameter m is

$$a \uparrow ((bp)^c) - f \uparrow ((gp)^h) = \{a \uparrow [(b^m)((bp)^{c-m})] - f \uparrow [(g^m)((gp)^{h-m})\} \Pi(r = 0, m - 1) \{\Sigma(s = 0, p - 1)[a \uparrow (bs((bp)^{c-1-r}))](b \uparrow r)] [f \uparrow (g(p - 1 - s)((gp)^{h-1-r})(g \uparrow r))]\}.$$

Proof. Consider the identity

$$\gamma \uparrow (p^m) - \delta \uparrow (p^m) = (\gamma \uparrow (p^{m-1}) - \delta \uparrow (p^{m-1})) \{\Sigma(s = 0, p - 1)[(\gamma \uparrow (p^{m-1})) \uparrow s][(\delta \uparrow (p^{m-1})) \uparrow (p - 1 - s)]\}.$$

The term $(\gamma \uparrow (p^{m-1}) - \delta \uparrow (p^{m-1}))$ can be replaced for an n th general recursion to give

$$\gamma \uparrow (p^m) - \delta \uparrow (p^m) = (\gamma \uparrow (p^{m-1-n}) - \delta \uparrow (p^{m-1-n})) \Pi(r = 0, n) \{\Sigma(s = 0, p - 1) [(\gamma \uparrow (p^{m-1-r})) \uparrow s][(\delta \uparrow (p^{m-1-r})) \uparrow (p - 1 - s)]\}.$$

Hence allocating the maximum n th replacement to $m - 1$, our star equation is

$$(*) \quad \gamma \uparrow (p^m) - \delta \uparrow (p^m) = [\gamma - \delta] \Pi(r = 0, m - 1) \{\Sigma(s = 0, p - 1) [(\gamma \uparrow (p^{m-1-r})) \uparrow s][(\delta \uparrow (p^{m-1-r})) \uparrow (p - 1 - s)]\}.$$

Put

$$\alpha = a \uparrow ((bp)^c) = \gamma \uparrow (p^m),$$

leading to

$$\gamma = \gamma \uparrow (p \uparrow 0) = \gamma \uparrow [(p^m)(p^{-m})] = [\gamma \uparrow p^m] \uparrow (p^{-m}) = \alpha \uparrow (p^{-m}).$$

Now, as can be confirmed by multiplying both sides by $(b \uparrow -m)$,

$$p \uparrow -m = (bp)^{-m} b^m,$$

so

$$\gamma = a \uparrow [b^m((bp)^{c-m})].$$

If we likewise allocate

$$\beta = f \uparrow (gp)^h = \delta \uparrow (p^m),$$

reducing to

$$\delta = \beta \uparrow (p^{-m})$$

then we obtain similarly

$$\delta = f \uparrow [g^m ((gp)^{h-m})].$$

In consequence

$$\begin{aligned} a \uparrow ((bp)^c) - f \uparrow ((gp)^h) = \\ \{ a \uparrow [b^m (bp)^{c-m}] - f \uparrow [g^m (gp)^{h-m}] \} \\ \Pi(r=0, m-1) \{ \Sigma(s=0, p-1) \\ [(\alpha \uparrow (p^{-1-r})) \uparrow s][(\beta \uparrow (p^{-1-r})) \uparrow (p-1-s)] \}. \end{aligned}$$

For the first of the last two terms in [], assign

$$\alpha = a \uparrow ((bp)^c)$$

and

$$p^{-1-r} = [(bp)^{-1-r}][b^{1+r}].$$

Then this term is

$$\{ a \uparrow [bs[(bp)^{c-1-r}]b^r] \}$$

and the second term is by similar process

$$\{ f \uparrow [g(p-1-s)[(gp)^{h-1-r}]g^r] \}. \blacksquare$$

The *first Fermat addition factorisation theorem (first FAFT)* states:

Let $g, p \in \mathbf{N}$ be odd numbers and $h \in \mathbf{N}$. Then

$$\begin{aligned} a \uparrow ((bp)^c) + f \uparrow ((gp)^h) = \\ \{ (a \uparrow [(bp)^{c-1}])^b + (f \uparrow [(gp)^{h-1}])^g \} \{ \Sigma(s=0, p-1) \\ [(a \uparrow [(bp)^{c-1}]) \uparrow bs][((-f) \uparrow [(gp)^{h-1}]) \uparrow g(p-1-s)] \}. \end{aligned}$$

Proof. Introducing

$$\alpha = \gamma^p, \beta = \delta^p,$$

we revisit the *first FSFT* equation

$$\alpha - \beta = [\alpha^{1/p} - \beta^{1/p}] \{ \Sigma(s=0, p-1)[(\alpha^{s/p})[\beta^{1-1/p-s/p}]] \}.$$

Using

$$\alpha = a \uparrow (bp)^c = a \uparrow [(bp)^1 (bp)^{c-1}] = (a \uparrow [(bp)^{c-1}]) \uparrow bp$$

and similarly

$$\beta = f \uparrow (gp)^h = (f \uparrow [(gp)^{h-1}]) \uparrow gp$$

gives, under the transformation $\beta \rightarrow -\beta$, that $\beta^{1/p}$ changes sign as $\delta \rightarrow -\delta$, since p is odd, which transforms $f \rightarrow -f$, since gp is odd in $\beta = f \uparrow (gp)^h$. Hence the result. \blacksquare

The *second Fermat addition factorisation theorem (second FAFT)* for free parameter m states:

Let g and $p \in \mathbf{N}$ be odd numbers and $h \in \mathbf{N}$. Then

$$\begin{aligned} a \uparrow ((bp)^c) + f \uparrow ((gp)^h) = \\ \{ a \uparrow [(b^m)(bp)^{c-m}] + f \uparrow [(g^m)(gp)^{h-m}] \} \\ \Pi(r=0, m-1) \{ \Sigma(s=0, p-1)[a \uparrow (bs[(bp)^{c-1-r}]b^r)] \\ [(-f) \uparrow (g(p-1-s)[(gp)^{h-1-r}]g^r)] \}. \end{aligned}$$

Proof. The conditions are identical to the *first FAFT*, and the proof follows by close analogy with the *second FSFT* proof. In particular, we note the following result, suitably amended, i.e. we have performed the transformation $\delta \rightarrow -\delta$.

$$\begin{aligned} (**) \quad \gamma \uparrow (p \uparrow m) + \delta \uparrow (p \uparrow m) = [\gamma + \delta] \Pi(r=0, m-1) \{ \Sigma(s=0, p-1) \\ [(\gamma \uparrow [p \uparrow (m-1-r)]) \uparrow s][(-\delta) \uparrow [p \uparrow (m-1-r)]) \uparrow (p-1-s)] \}. \blacksquare \end{aligned}$$

We subsequently identify $\varepsilon, \eta, \theta \in \mathbf{C}$ as complex numbers, $e = 2.718\dots$ and $i = \sqrt{-1}$. We now relax our conditions, to allow complex arithmetic *on*, but not further non-real operations *within*, for example, $a \uparrow b = e \uparrow (i\pi q/p)$ terms. A way of doing this is to consider $a \uparrow b$ expressions as scalars and complex numbers as vectors. This is an idea found in K theory.

We have stated that our factorisation theorems give unique factorisation when applied to natural numbers up to order of factors.

For complex cyclotomics as used in the next lemma, uniqueness of factorisation depends on the class number [30]. That is why, in section 3 on prime number and factorisation theorems, we prefer to use formulae developed for the real case.

The next *FAFT* theorems have *FSFT* analogues. Here is *Lemma 1*.

$$\gamma^p + \delta^p = \Pi(s = 0, p - 1)[\gamma - \delta(e \uparrow i\pi(2s + 1)/p)].$$

Proof. We first note that the leading term in the expansion is γ^p . The trailing term is $(-\delta)^p(e \uparrow i\pi[\Sigma(s = 0, p - 1)(2s + 1)/p])$.

Now the following arithmetic series sum has the value

$$\Sigma(s = 0, p - 1)s = p(p - 1)/2,$$

so the Σ summation in [] above is

$$[2(p(p - 1)/2) + p]/p = p.$$

Hence, irrespective of whether p is even or odd, since $e \uparrow i\pi(2s + 1) = -1$, the trailing term is δ^p .

Now consider the n th term in the expansion. If $n \neq 0$ or $p - 1$, it consists of a *summation*

$$\Sigma(r = 0, m)\varepsilon_r \gamma^{p-n} \delta^n$$

each ε_r is the product of n factors $(e \uparrow i\pi(2t + 1)/p)$, where the product terms range over all combinations of t from 0 to $p - 1$. If $\Sigma_r \varepsilon_r \neq 0$, it consists of a non-zero vector in the complex plane. Permute the roots under the cyclic transformation $s \rightarrow s + 1$. Then $\varepsilon_r \rightarrow (e \uparrow 2\pi i/p)\varepsilon_r \neq \varepsilon_r$, and $\Sigma_r \varepsilon_r$ remains the same, since it consists of the sum of *all* combinations. The rotation of roots implies the complex sum vector must also be rotated by an ε_r multiplication $\neq 1$, a contradiction unless the sum is zero. ■

The *third Fermat addition factorisation theorem (third FAFT)* is

$$a \uparrow ((bp)^c) + f \uparrow ((gp)^h) = \Pi(s = 0, p - 1) \{(a \uparrow [(bp)^{c-1}])^b - (f \uparrow [(gp)^{h-1}])^g (e \uparrow i\pi(2s + 1)/p)\}.$$

Proof. Put

$$\alpha = \gamma^p, \beta = \delta^p.$$

Then using *lemma 1*, we obtain

$$\alpha + \beta = \Pi(s = 0, p - 1)[\alpha^{1/p} - \beta^{1/p}(e \uparrow i\pi(2s + 1)/p)]$$

and with the substitutions

$$\alpha = a \uparrow (bp \uparrow c) = a \uparrow [(bp \uparrow 1)(bp \uparrow (c - 1))] = (a \uparrow [bp \uparrow (c - 1)]) \uparrow bp$$

and

$$\beta = f \uparrow (gp \uparrow h) = (f \uparrow [gp \uparrow (h - 1)]) \uparrow gp,$$

this results in the theorem. ■

Lemma 2. Let $p = j(2 \uparrow k)$ with j odd and k non-negative. Then

$$e \uparrow (i\pi(2s + 1)/p) = (-1) \uparrow (1/p) = \sqrt[p]{-1}$$

has a real root (which is -1) only for $k = 0$.

Proof. Let $k = 0$, so p is an odd number. By applying $\uparrow(1/p)$ to the equations below

$$-1 = (-1) \uparrow p$$

is a solution, for p odd, so $\sqrt[p]{-1}$ has a real root, -1 . If $k \neq 0$, then p is even, implying

$$-1 \neq (-1) \uparrow p \text{ and } -1 \neq 1 \uparrow p.$$

The norm of the root is 1, so there are no real root of -1 possibilities for p even. ■

The *fourth Fermat addition factorisation theorem (fourth FAFT)* states:

Let $p \in \mathbf{N}$ be an odd number. Then for free parameter m

$$\begin{aligned} a \uparrow ((bp)^c) + f \uparrow ((gp)^h) = \\ \{ a \uparrow [(b^m)(bp)^{c-m}] + f \uparrow [(g^m)(gp)^{h-m}] \} \\ \Pi(r = 0, m - 1) \{ \Pi(s = 0, p - 1, \text{omit } (p - 1)/2) \\ [(a \uparrow (b[(bp)^{c-1-r}]b^r)) \\ - (f \uparrow (g[(gp)^{h-1-r}]g^r)) (e \uparrow i\pi(2s + 1)/p)] \}. \end{aligned}$$

Proof. Consider the following factorisation identity, beginning with the ‘real root’ case, which corresponds to $s = (p - 1)/2$, so by *lemma 2*, p is odd:

$$\begin{aligned} \gamma \uparrow (p \uparrow m) + \delta \uparrow (p \uparrow m) = \{ \gamma \uparrow (p \uparrow (m - 1)) + \delta \uparrow (p \uparrow (m - 1)) \} \\ \Pi(s = 0, p - 1, \text{omit } (p - 1)/2) \\ [\gamma \uparrow (p \uparrow (m - 1)) - [\delta \uparrow (p \uparrow (m - 1))] (e \uparrow i\pi(2s + 1)/p)]. \end{aligned}$$

The term $\{ \gamma \uparrow (p \uparrow (m - 1)) + \delta \uparrow (p \uparrow (m - 1)) \}$ can be replaced for an n th general recursion to give

$$\begin{aligned} \gamma \uparrow (p \uparrow m) + \delta \uparrow (p \uparrow m) = \{ \gamma \uparrow [p \uparrow (m - 1 - n)] + \delta \uparrow [p \uparrow (m - 1 - n)] \} \\ \Pi(r = 0, n) [\Pi(s = 0, p - 1, \text{omit } (p - 1)/2) \\ \{ \gamma \uparrow [p \uparrow (m - 1 - r)] - (\delta \uparrow [p \uparrow (m - 1 - r)]) (e \uparrow i\pi(2s + 1)/p) \}]. \end{aligned}$$

Hence allocating the maximum n th replacement to $m - 1$, our equation is

$$\begin{aligned} \gamma \uparrow (p \uparrow m) + \delta \uparrow (p \uparrow m) = [\gamma + \delta] \Pi(r = 0, m - 1) \{ \Pi(s = 0, p - 1, \text{omit } (p - 1)/2) \\ \{ \gamma \uparrow [p \uparrow (m - 1 - r)] - (\delta \uparrow [p \uparrow (m - 1 - r)]) (e \uparrow i\pi(2s + 1)/p) \} \}. \end{aligned}$$

Our substitutions now follow the steps of the *second FSFT*. Put

$$\alpha = a \uparrow (bp \uparrow c) = \gamma \uparrow (p \uparrow m).$$

We recall this leads to

$$\gamma = \alpha \uparrow (p \uparrow -m) = \alpha \uparrow [(bp \uparrow -m)(b \uparrow m)] = a \uparrow [(b \uparrow m)(bp \uparrow (c - m))].$$

If we likewise allocate

$$\beta = f \uparrow (gp \uparrow h) = \delta \uparrow (p \uparrow m),$$

then we obtain similarly

$$\delta = f \uparrow [(g \uparrow m)(gp \uparrow (h - m))].$$

Consequently

$$\begin{aligned} a \uparrow (bp \uparrow c) + f \uparrow (gp \uparrow h) = \\ \{ a \uparrow [(b \uparrow m)(bp \uparrow (c - m))] + f \uparrow [(g \uparrow m)(gp \uparrow (h - m))] \} \\ \Pi(r = 0, m - 1) \{ \Pi(s = 0, p - 1, \text{omit } (p - 1)/2) \\ [(\alpha \uparrow [p \uparrow (-1 - r)]) - (\beta \uparrow [p \uparrow (-1 - r)]) (e \uparrow i\pi(2s + 1)/p)] \}. \end{aligned}$$

For the first term of the last expression in [], assign

$$\alpha = a \uparrow (bp \uparrow c)$$

and

$$p \uparrow (-1 - r) = [bp \uparrow (-1 - r)](b \uparrow (1 + r)).$$

Then this term is

$$\{a \uparrow (b[bp \uparrow (c - 1 - r)](b \uparrow r))\}$$

and in comparable manner the second term is

$$\{(f \uparrow (g[gp \uparrow (h - 1 - r)](g \uparrow r)))(e \uparrow i\pi(2s + 1)/p)\}. \blacksquare$$

Under the *FAFT* constraints, say p odd, each of the *FAFT* and *FSFT* equations is equivalent by “if and only if” equivalence to the identity $(\gamma, \delta) = (\gamma, \delta)$, so under *FAFT* constraints their equaliser (intersection) is also equivalent to this identity. Thus we can also form linear combinations of *FAFT* and *FSFT* equations. These theorems we call *linear combination factorisation theorems – LCFT*. Here is a typical example.

Let g and $p \in \mathbf{N}$ be odd, $h \in \mathbf{N}$. Put

$$A = a \uparrow [(b^m)(bp)^{c-m}]$$

$$B = f \uparrow [(g^m)(gp)^{h-m}]$$

$$C_r = \Sigma(s = 0, (p - 1)/2) \{a \uparrow (2bs[(bp)^{c-1-r}]b^r) \{f \uparrow (g(p - 1 - 2s)[(gp)^{h-1-r}]g^r)\}$$

$$D_r = \Sigma(s = 0, (p - 3)/2) \{a \uparrow (b(2s + 1)[(bp)^{c-1-r}]b^r) \{f \uparrow (g(p - 2 - 2s)[(gp)^{h-1-r}]g^r)\}.$$

Then

$$\eta[a \uparrow ((bp)^c)] + \theta[f \uparrow ((gp)^h)] = \frac{1}{2}[(\eta + \theta)(A + B) \Pi(r = 0, m - 1)(C_r - D_r) + (\eta - \theta)(A - B) \Pi(r = 0, m - 1)(C_r + D_r)]. \blacksquare$$

Our formula for difference of powers may be generalised by putting $q = jk$ and

$$\gamma^q - \delta^q = [(\gamma \uparrow k) - (\delta \uparrow k)] \{ \Sigma(s = 0, j - 1) [\gamma \uparrow ks] [\delta \uparrow k(j - 1 - s)] \}.$$

Accordingly, with $j = 2^n$, ω_{2j} a primitive $2j$ th root of unity and k odd

$$\gamma^q + \delta^q = [(\gamma \uparrow k) + (\omega_{2j}\delta) \uparrow k] \{ \Sigma(s = 0, j - 1) [\gamma \uparrow ks] [(-\omega_{2j}\delta) \uparrow k(j - 1 - s)] \},$$

or with the same $j = 2^n$ and k odd

$$\gamma^q + \delta^q = [(\gamma \uparrow 2^n) + (\delta \uparrow 2^n)] \{ \Sigma(s = 0, k - 1) [\gamma \uparrow 2^ns] [(-\delta \uparrow 2^n) \uparrow (k - 1 - s)] \}.$$

This can be compared with the binomial identity

$$\gamma^q + \delta^q = [(\gamma \uparrow k) + (\delta \uparrow k)]^j - \{ \Sigma(s = 1, j - 1) [(j - 1)!/s!(j - 1 - s)!] [\gamma \uparrow ks] [\delta \uparrow k(j - 1 - s)] \}. \blacksquare$$

Thus for q even as above an option is

$$Z = \eta(\gamma^q) + \theta(\delta^q) = \frac{1}{2}[(\eta + \theta)(\gamma \uparrow [2^n] + \delta \uparrow [2^n])U + (\eta - \theta)(\gamma \uparrow [2^n] - \delta \uparrow [2^n])V],$$

with

$$U = \Sigma(s = 0, k - 1) [\gamma \uparrow (2^ns)] \{ [(-\delta \uparrow 2^n) \uparrow (k - 1 - s)] \}$$

and

$$V = \Sigma(s = 0, k - 1) [\gamma \uparrow (2^ns)] \{ \delta \uparrow [2^n(k - 1 - s)] \}. \blacksquare$$

The general *LCFT* formula for any p is then

$$Z = \frac{1}{2}[(1 - (-1)^p)(\text{formula for odd } p) + (1 + (-1)^p)(\text{formula for even } p)]. \blacksquare$$

2.3 Extension of the LCFT to many variables.

We now give a modified example of the *LCFT* (note that here firstly, p is odd)

$$Z = \eta(\gamma \uparrow p) + \theta(\delta \uparrow p) = \frac{1}{2}[(\eta + \theta)(\gamma + \delta)X + (\eta - \theta)(\gamma - \delta)Y],$$

generated from essentially γ replaced by the sum of variables $\Sigma(i = 0, n - 1)\gamma_i$, and δ replaced by the sum $\Sigma(i = 0, n - 1)\delta_i$. This is suitably general, because if, for example, there are less variables δ_i than γ_i , say j of them, we can set δ_i to zero for $j \leq i < n - 1$. We will first give an example restricted to the case $n = 3$.

The *multinomial theorem* is

$$(\gamma_0 + \gamma_1 + \dots + \gamma_{n-1})^p = \Sigma p! / (p_0! p_1! \dots p_{n-1}!) [(\gamma_0 \uparrow p_0) \dots (\gamma_{n-1} \uparrow p_{n-1})],$$

where the sum is extended over all non-negative p_i with $\Sigma p_i = p$.

For example, if $n = 3 = p$, then

$$\begin{aligned} (\gamma_0 + \gamma_1 + \gamma_2)^3 &= (\gamma_0^2 + 3\gamma_1^2 + 3\gamma_2^2)\gamma_0 + (\gamma_1^2 + 3\gamma_2^2 + 3\gamma_0^2)\gamma_1 + (\gamma_2^2 + 3\gamma_0^2 + 3\gamma_1^2)\gamma_2 \\ &\quad + 6\gamma_0\gamma_1\gamma_2. \end{aligned}$$

Let p be odd. Then the expansion of

$$(\gamma_0 + \gamma_1 + \dots + \gamma_{n-1})^p$$

can be written as a sum

$$\Sigma_{y, \text{combinations for } y} J_r \dots J_x (\gamma_r \dots \gamma_x)$$

where the number of terms in the sequence r, \dots, x is y , with y odd $\leq n$ and each coefficient $J_r \dots J_x$ is invariant under any transformation $\gamma_s \rightarrow -\gamma_s$, $r \geq s \geq x$.

Proof. Each term in the expansion is a scalar, α , times a product $\Pi_t \gamma_t^q$, with $\Sigma q = p$, p odd. This may be represented by $\alpha \Pi_j \gamma_j^u \Pi_k \gamma_k^v$, with u even and v odd. Hence it may be represented by even parity terms invariant under $\gamma_s \rightarrow -\gamma_s$ given by $\alpha \Pi_j \gamma_j^u \Pi_k \gamma_k^{v-1}$, each multiplied by odd parity terms $(\gamma_r \dots \gamma_x) = \Pi_k \gamma_k$. Collecting together all the even parity terms, we put

$$J_r \dots J_x = \Sigma_i \alpha_i \Pi_j \gamma_j^u \Pi_k \gamma_k^{v-1}.$$

If there exists any term $J_r \dots J_x \Pi_k \gamma_k$, where k ranges over an even number of values, then $J_r \dots J_x = \Sigma_i \alpha_i \Pi_k \gamma_k^w$, where Σw is even for each i , since $J_r \dots J_x$ is of even parity, which contradicts for each i that $p = \Sigma w +$ the range of k values, is odd. Hence $y =$ the range of k values, is odd. ■

If $p \geq n$, with p, n odd, then the number of $J_r \dots J_x$ terms is 2^{n-1} . If $p < n$, the number of terms is

$$\Sigma(k = 0, (p-1)/2) [n! / (2k+1)! (n-2k-1)!].$$

Proof. If $p \geq n$, then the number of terms is the number of combinations of odd $\gamma_r \dots \gamma_x$

$$\begin{aligned} &= n + n(n-1)(n-2)/2.3 + \dots + n! / (2k+1)! (n-2k-1)! + \dots + 1 \\ &= \frac{1}{2}(1+1)^n = 2^{n-1}. \end{aligned}$$

If $p < n$, n odd, it is the same series truncated after the $\frac{1}{2}(p+1)$ th term. ■

Consider for $n = 3$, p odd,

$$\begin{aligned} (\gamma_0 + \gamma_1 + \gamma_2)^p - (\delta_0 + \delta_1 + \delta_2)^p &= [\gamma_0 + \gamma_1 + \gamma_2 - \delta_0 - \delta_1 - \delta_2] \\ &\quad [\Sigma(s = 0, p-1) [(\gamma_0 + \gamma_1 + \gamma_2) \uparrow s] [(\delta_0 + \delta_1 + \delta_2) \uparrow (p-1-s)]], \end{aligned}$$

which by the above theorem can be equated to

$$J_0\gamma_0 + J_1\gamma_1 + J_2\gamma_2 + J_{012}\gamma_0\gamma_1\gamma_2 + K_0\delta_0 + K_1\delta_1 + K_2\delta_2 + K_{012}\delta_0\delta_1\delta_2,$$

where if p were = 1 then we would have $J_{012} = K_{012} = 0$.

We wish to add together the following combination

$$\begin{aligned} & a_0[(\gamma_0 + \gamma_1 + \gamma_2)^p - (\delta_0 + \delta_1 + \delta_2)^p] + a_1[(-\gamma_0 + \gamma_1 + \gamma_2)^p - (\delta_0 + \delta_1 + \delta_2)^p] \\ & a_2[(\gamma_0 - \gamma_1 + \gamma_2)^p - (\delta_0 + \delta_1 + \delta_2)^p] + b_0[(\gamma_0 + \gamma_1 + \gamma_2)^p - (-\delta_0 - \delta_1 - \delta_2)^p] \\ & b_1[(\gamma_0 + \gamma_1 + \gamma_2)^p - (\delta_0 - \delta_1 - \delta_2)^p] + b_2[(\gamma_0 + \gamma_1 + \gamma_2)^p - (-\delta_0 + \delta_1 - \delta_2)^p]. \end{aligned}$$

This linear combination may be equated to

$$\begin{aligned} & \eta_0 J_0 \gamma_0 + \eta_1 J_1 \gamma_1 + \eta_2 J_2 \gamma_2 + \eta_{012} J_{012} \gamma_0 \gamma_1 \gamma_2 + \\ & \theta_0 K_0 \delta_0 + \theta_1 K_1 \delta_1 + \theta_2 K_2 \delta_2 + \theta_{012} K_{012} \delta_0 \delta_1 \delta_2, \end{aligned}$$

where, for example,

$$\begin{aligned} J_0 \gamma_0 &= (-J_0)(-\gamma_0) \\ J_{012} \gamma_0 \gamma_1 \gamma_2 &= (-J_{012})(-\gamma_0)(-\gamma_1)(-\gamma_2), \end{aligned}$$

giving

$$\begin{aligned} \eta_0 &= a_0 - a_1 + a_2 + b_0 + b_1 + b_2 \\ \eta_1 &= a_0 + a_1 - a_2 + b_0 + b_1 + b_2 \\ \eta_2 &= a_0 + a_1 + a_2 + b_0 + b_1 + b_2 \\ -\theta_0 &= a_0 + a_1 + a_2 - b_0 + b_1 - b_2 \\ -\theta_1 &= a_0 + a_1 + a_2 - b_0 - b_1 + b_2 \\ -\theta_2 &= a_0 + a_1 + a_2 - b_0 - b_1 - b_2. \end{aligned}$$

We also have the supplementary equations

$$\begin{aligned} \eta_{012} &= a_0 - a_1 - a_2 + b_0 + b_1 + b_2 \\ -\theta_{012} &= a_0 + a_1 + a_2 - b_0 + b_1 + b_2. \end{aligned}$$

A little linear algebra then gives

$$\begin{aligned} a_1 &= (\eta_2 - \eta_0)/2, \\ a_2 &= (\eta_2 - \eta_1)/2 \end{aligned}$$

and

$$a_0 = (\eta_0 + \eta_1 - \eta_2 - \theta_2)/2.$$

Likewise

$$\begin{aligned} b_1 &= (\theta_2 - \theta_0)/2, \\ b_2 &= (\theta_2 - \theta_1)/2 \end{aligned}$$

and

$$b_0 = (\theta_0 + \theta_1 - \theta_2 + \eta_2)/2.$$

These results, easily extended to many variables, imply

$$\eta_{012} = \eta_0 + \eta_1 - \eta_2$$

and

$$\theta_{012} = \theta_0 + \theta_1 - \theta_2.$$

We can express $J_0\gamma_0$, $J_1\gamma_1$, $J_2\gamma_2$ and $J_{012}\gamma_0\gamma_1\gamma_2$ in terms of $(\gamma_0 + \gamma_1 + \gamma_2)^p$.

$$\begin{aligned} J_0\gamma_0 &= \frac{1}{4}[(\gamma_0 + \gamma_1 + \gamma_2)^p - (-\gamma_0 + \gamma_1 + \gamma_2)^p + (\gamma_0 - \gamma_1 + \gamma_2)^p + (\gamma_0 + \gamma_1 - \gamma_2)^p]. \\ J_1\gamma_1 &= \frac{1}{4}[(\gamma_0 + \gamma_1 + \gamma_2)^p + (-\gamma_0 + \gamma_1 + \gamma_2)^p - (\gamma_0 - \gamma_1 + \gamma_2)^p + (\gamma_0 + \gamma_1 - \gamma_2)^p]. \end{aligned}$$

$$J_2\gamma_2 = \frac{1}{4}[(\gamma_0 + \gamma_1 + \gamma_2)^p + (-\gamma_0 + \gamma_1 + \gamma_2)^p + (\gamma_0 - \gamma_1 + \gamma_2)^p - (\gamma_0 + \gamma_1 - \gamma_2)^p].$$

$$J_{012}\gamma_0\gamma_1\gamma_2 = \frac{1}{4}[(\gamma_0 + \gamma_1 + \gamma_2)^p - (-\gamma_0 + \gamma_1 + \gamma_2)^p - (\gamma_0 - \gamma_1 + \gamma_2)^p - (\gamma_0 + \gamma_1 - \gamma_2)^p].$$

We now introduce the symbol $X_{uvw,xyz}$, in which u is 0 if γ_0 is positive, and u is 1 if γ_0 is negative, and similarly with v for γ_1 and w for γ_2 . We adopt a similar type of convention for x, y, z with respect to δ_0, δ_1 and δ_2 . Thus we have the expression for p odd

$$(\gamma_0 + \gamma_1 + \gamma_2)^p - (\delta_0 + \delta_1 + \delta_2)^p = [\gamma_0 + \gamma_1 + \gamma_2 - \delta_0 - \delta_1 - \delta_2]X_{000,000},$$

with

$$X_{000,000} = [\sum(s=0, p-1)(\gamma_0 + \gamma_1 + \gamma_2)^{\uparrow s}][(\delta_0 + \delta_1 + \delta_2)^{\uparrow(p-1-s)}].$$

Hence we have the following *theorem*.

$$\begin{aligned} & \eta_0 J_0 \gamma_0 + \eta_1 J_1 \gamma_1 + \eta_2 J_2 \gamma_2 + (\eta_0 + \eta_1 - \eta_2) J_{012} \gamma_0 \gamma_1 \gamma_2 + \\ & \theta_0 K_0 \delta_0 + \theta_1 K_1 \delta_1 + \theta_2 K_2 \delta_2 + (\theta_0 + \theta_1 - \theta_2) K_{012} \delta_0 \delta_1 \delta_2 \\ & = \frac{1}{2} [(\eta_0 + \eta_1 - \eta_2 - \theta_2)(\gamma_0 + \gamma_1 + \gamma_2 - \delta_0 - \delta_1 - \delta_2)X_{000,000} \\ & + (\eta_2 - \eta_0)(-\gamma_0 + \gamma_1 + \gamma_2 - \delta_0 - \delta_1 - \delta_2)X_{100,000} \\ & + (\eta_2 - \eta_1)(\gamma_0 - \gamma_1 + \gamma_2 - \delta_0 - \delta_1 - \delta_2)X_{010,000} \\ & + (\theta_0 + \theta_1 - \theta_2 + \eta_2)(\gamma_0 + \gamma_1 + \gamma_2 + \delta_0 + \delta_1 + \delta_2)X_{000,111} \\ & + (\theta_2 - \theta_0)(\gamma_0 + \gamma_1 + \gamma_2 - \delta_0 + \delta_1 + \delta_2)X_{000,011} \\ & + (\theta_2 - \theta_1)(\gamma_0 + \gamma_1 + \gamma_2 + \delta_0 - \delta_1 + \delta_2)X_{000,101}]. \blacksquare \end{aligned}$$

Consider the general case for p odd

$$(\sum(i=0, n-1)\gamma_i)^p - (\sum(i=0, n-1)\delta_i)^p = [\sum(i=0, n-1)(\gamma_i - \delta_i)]$$

$$[\sum(s=0, p-1)(\sum(i=0, n-1)\gamma_i)^{\uparrow s}][(\sum(i=0, n-1)\delta_i)^{\uparrow(p-1-s)}],$$

which by the above theorem can be equated to

$$\sum_{y, \text{combinations for } y} J_r \dots x (\gamma_r \dots \gamma_x) - \sum_{y, \text{combinations for } y} K_r \dots x (\delta_r \dots \delta_x),$$

where we have introduced $K_r \dots x$ for the coefficient of $(\delta_r \dots \delta_x)$ similar to $J_r \dots x$ for $(\gamma_r \dots \gamma_x)$.

If $p < n$, then for $y > p$, $J_r \dots x = K_r \dots x = 0$.

We wish now to add together linear combinations of $2n$ independent equations, each of a type similar to the above, expressed in the n variables γ_i and the n variables δ_i .

Define the symbol $\xi(i,j)$ by

$$\begin{aligned} \xi(i,j) &= 1 \text{ for } i = j \\ &= 0 \text{ for } i \neq j. \end{aligned}$$

Then our general linear combination is

$$\begin{aligned} & \sum(s=0, n-1)[a_s(\sum(r=0, n-1)(\gamma_r - 2\xi(s,r-1)\gamma_{r-1}))^p - (\sum(r=0, n-1)\delta_r)^p] \\ & + \sum(s=0, n-1)[b_s(\sum(r=0, n-1)\gamma_r)^p - (\sum(r=0, n-1)(-\delta_r + 2\xi(s,r-1)\delta_r))^p]. \end{aligned}$$

With y odd, our linear combination equals

$$\sum_{y, \text{combinations for } y} \eta_r \dots x J_r \dots x (\gamma_r \dots \gamma_x) + \sum_{y, \text{combinations for } y} \theta_r \dots x K_r \dots x (\delta_r \dots \delta_x),$$

where

$$\begin{aligned} J_r \dots x (\gamma_r \dots \gamma_x) &= -J_r \dots x [(-\gamma_r) \dots (-\gamma_x)], \\ K_r \dots x (\delta_r \dots \delta_x) &= -K_r \dots x [(-\delta_r) \dots (-\delta_x)]. \end{aligned}$$

This gives

$$\eta_r = \Sigma(s = 0, n - 1)[a_s - 2\xi(r + 1, s)a_{r+1} + b_s]$$

and

$$-\theta_r = \Sigma(s = 0, n - 1)[a_s - b_s + 2\xi(r + 1, s)b_{r+1}].$$

Introducing, say, $\eta(012)$ for η_{012} , we also have the supplementary equations

$$\eta(r_0 \dots r_{y-1}) = \Sigma(s = 0, n - 1)[a_s - 2\Sigma(t = 0, y - 1)\xi(r_{t+1}, s)a_{t+1} + b_s]$$

$$-\theta(r_0 \dots r_{y-1}) = \Sigma(s = 0, n - 1)[a_s - b_s + 2\Sigma(t = 0, y - 1)\xi(r_{t+1}, s)b_{t+1}],$$

where we consider the set of variables $(r_0 \dots r_{y-1})$ to be any suitable combination for y .

Applying linear algebra, where s goes from 0 to $n - 2$, we obtain

$$a_{s+1} = (\eta_{n-1} - \eta_s)/2,$$

$$a_0 = ((-n + 2)\eta_{n-1} + \Sigma(s = 0, n - 2)\eta_s - \theta_{n-1})/2.$$

Likewise

$$b_{s+1} = (\theta_{n-1} - \theta_s)/2,$$

$$b_0 = ((-n + 2)\theta_{n-1} + \Sigma(s = 0, n - 2)\theta_s + \eta_{n-1})/2.$$

These results imply

$$\eta(r_0 \dots r_{y-1}) = \frac{1}{2}[(-n + 4)\eta_{n-1} + (-n + 2)\theta_{n-1}] - \Sigma(s = 0, n - 1)[\Sigma(t = 0, y - 1)\xi(r_{t+1}, s)(\eta_{n-1} - \eta_t)].$$

$$-\theta(r_0 \dots r_{y-1}) = \frac{1}{2}[(n - 4)\theta_{n-1} + (-n + 2)\eta_{n-1}] + \Sigma(s = 0, n - 1)[\Sigma(t = 0, y - 1)\xi(r_{t+1}, s)(\theta_{n-1} - \theta_t)].$$

$J_r \dots x(\gamma_r \dots \gamma_x)$ can then be computed explicitly.

We now introduce the symbol $X(v_0v_1 \dots v_{n-1}, x_0x_1 \dots x_{n-1})$, in which v_i is 0 if γ_i is positive, and v_i is 1 if γ_i is negative, and likewise for x_i with respect to δ_i . Thus we have the expression

$$\begin{aligned} & (\Sigma(s = 0, n - 1)\gamma_s)^p - (\Sigma(s = 0, n - 1)\delta_s)^p = \\ & [\Sigma(s = 0, n - 1)\gamma_s - \Sigma(s = 0, n - 1)\delta_s]X(0 \dots 0, 0 \dots 0) \end{aligned}$$

with

$$\begin{aligned} X(0 \dots 0, 0 \dots 0) = \\ \Sigma(r = 0, p - 1)[(\Sigma(s = 0, n - 1)\gamma_s)^{\uparrow r}][(\Sigma(s = 0, n - 1)\delta_s)^{\uparrow(p - 1 - r)}]. \end{aligned}$$

Writing, say, $J(012)$ for J_{012} and $\gamma(0)$ for γ_0 , we have the following *theorem*.

$$\begin{aligned} & \Sigma_{y, \text{combinations for } y} \eta(r_0 \dots r_{y-1})J(r_0 \dots r_{y-1})(\gamma(r_0) \dots \gamma(r_{y-1})) \\ & + \Sigma_{y, \text{combinations for } y} \theta(r_0 \dots r_{y-1})K(r_0 \dots r_{y-1})(\delta(r_0) \dots \delta(r_{y-1})) \\ & = \Sigma_{y, \text{combinations for } y} \frac{1}{2}[(-n + 4)\eta_{n-1} + (-n + 2)\theta_{n-1} - 2\Sigma(s = 0, n - 1) \\ & \quad [\Sigma(t = 0, y - 1)\xi(r_{t+1}, s)(\eta_{n-1} - \eta_t)]] \\ & \quad [\Sigma(s = 0, n - 1)[(1 - 2v_s)\gamma_s - \delta_s]X(v_0v_1 \dots v_{n-1}, 0 \dots 0)] \\ & - \Sigma_{y, \text{combinations for } y} \frac{1}{2}[(n - 4)\theta_{n-1} + (-n + 2)\eta_{n-1} + 2\Sigma(s = 0, n - 1) \\ & \quad [\Sigma(t = 0, y - 1)\xi(r_{t+1}, s)(\theta_{n-1} - \theta_t)]] \\ & \quad [\Sigma(s = 0, n - 1)[\gamma_s + (1 - 2x_s)\delta_s]X(0 \dots 0, x_0x_1 \dots x_{n-1})]. \blacksquare \end{aligned}$$

If q is even $= (2^n)k$, with k odd, then a formula for even q is obtained from the above formula under the transformation $p \rightarrow k$, $\gamma_s \rightarrow \gamma_s \uparrow 2^n$, $\delta_s \rightarrow \delta_s \uparrow 2^n$.

Alternatively, for q even, a complex cyclotomic formula can be utilised, where we set $q = jk = (2^n)k$, with k odd and ω_{2j} a primitive $2j$ th root of unity, obtainable from the above under the transformation $p \rightarrow j$, $\gamma_s \rightarrow \gamma_s \uparrow k$, $\delta_s \rightarrow (-\omega_{2j} \delta_s) \uparrow k$.

We recall, given $u = p$ or q , the general *LCFT* formula for Z is then

$$Z = \frac{1}{2} \{ [1 - (-1)^u] (\text{formula for } u \text{ odd}) + [1 + (-1)^u] (\text{formula for } u \text{ even}) \}. \blacksquare$$

3. Prime number, factorisation and divisibility theorems.

For γ or $\delta > 1 \in \mathbb{N}$, no representations of primes are of the form

$$\gamma^p + \delta^p,$$

except for the possibilities $p = 1$ or p a power of 2, the latter subsumed under $p = 2$.

Proof. Let p be odd. Then by (**), supposing the above expression is prime

$$\begin{aligned} \gamma \uparrow (p^m) + \delta \uparrow (p^m) &= [\gamma + \delta] \Pi(r = 0, m - 1) \\ &\{ \Sigma(s = 0, p - 1) [(\gamma \uparrow [p^{m-1-r}]) \uparrow s] [((-\delta) \uparrow [p^{m-1-r}]) \uparrow (p - 1 - s)] \}. \end{aligned}$$

Since the prime number and $\gamma + \delta$ are positive, so is the subsequent expression in [] which is a summation of integers, and $m = 1$, otherwise the expression factorises. Since $\gamma + \delta > 1$, the summation of integers is 1. This implies

$$\gamma^p + \delta^p = \gamma + \delta,$$

which is clearly only the case for $\gamma = \delta = 1$ or $p = 1$. Hence if $p \neq 1$, it is not odd.

Now if $p \neq 1$ is not a power of 2, there exists an odd factor $q \neq 1$ so that $p = kq$ and

$$(\gamma \uparrow k) \uparrow q + (\delta \uparrow k) \uparrow q$$

is prime, which we have proved is not the case. Hence $p = 1$, or $p = 2z$ is a power of 2, so all the latter such primes can be written as

$$(\gamma \uparrow z) \uparrow 2 + (\delta \uparrow z) \uparrow 2. \blacksquare$$

We note the following standard results, given e.g. in [3].

No prime of the form $4k + 3$ is a sum of two squares. ■

Any prime of the form $4k + 1$ can be represented uniquely (aside from the order of summands) as a sum of two squares. ■

Let p be odd, $\eta \neq \pm\theta \neq 0$ be integers, $\gamma \neq \delta \neq 0$ natural numbers,

$$X = \Sigma(s = 0, p - 1) [\gamma^s] [(-\delta)^{p-1-s}],$$

$$Y = \Sigma(s = 0, p - 1) [\gamma^s] [\delta^{p-1-s}]$$

and

$$Z = \eta(\gamma^p) + \theta(\delta^p) > 0.$$

If the product of $(\eta + \theta)$, $(\gamma + \delta)$ and X has two prime factors in common with the product $(\eta - \theta)$, $(\gamma - \delta)$ and Y , excluding at most one factor of ± 2 , then Z is not prime.

Proof. By the *LCFT*

$$\eta(\gamma^p) + \theta(\delta^p) = \frac{1}{2} [(\eta + \theta)(\gamma + \delta)X + (\eta - \theta)(\gamma - \delta)Y].$$

Hence under these conditions, for the expression to be prime, there are two distinct factors on the right hand side, one of which must be ± 2 . ■

We cannot modify these conditions by just reducing two prime factors down to *one*, because taking $p = 1$, $\eta = 5$, $\theta = -6$, $\gamma = 15$ and $\delta = 12$, then $Z = 3$ is prime, but we construct a proof of this modification under the further constraint $\eta \neq \theta \neq 0 \in \mathbf{N}$.

We mention related results. *When the expression*

$$\gamma^2 + \delta^2 = \frac{1}{2}[(\gamma + \delta)(\gamma + \delta) + (\gamma - \delta)(\gamma - \delta)]$$

is prime, then $\gamma - \delta$ does not share any prime factor with $\gamma + \delta$. ■

Any integer may be represented by $\pm Z$ (put, say, $\delta = 1$. We allow here $Z = 0$). ■

Let $\eta \neq \theta \neq 0$ and $\gamma \neq \delta \neq 0$ be natural numbers and p , X , Y and Z be as in the previous theorem. If the product of $(\gamma - \delta)$, $(\eta - \theta)$ and Y has a prime factor in common with the product $(\gamma + \delta)$, $(\eta + \theta)$ and X , excluding at most one factor of ± 2 for the pairings of $(\gamma - \delta)$ with $(\gamma + \delta)$ or $(\eta - \theta)$ with $(\eta + \theta)$, then Z is not prime.

Sketch of proof. If A and B have a prime common factor, we write $jA = kB$, where the common factor is $(A/k) = (B/j)$. We allocate j and k as positive where possible.

Let p be odd. Define $2W = Y - X$. We will need the following identities.

$$(\gamma + \delta)X = \gamma^p + \delta^p$$

and

$$\begin{aligned} \gamma X + (\gamma - \delta)W &= \gamma^p, \\ \delta X + (\delta - \gamma)W &= \delta^p. \end{aligned}$$

We immediately mention that for pairings of $(\gamma - \delta)$ with $(\gamma + \delta)$, for $p = 3$, $\eta = 1$, $\theta = 2$, $\gamma = 3$ and $\delta = 1$, that $Z = 29$ is prime, so the exclusion of at most one factor of ± 2 is necessary. The same goes for the pairing of $(\eta - \theta)$ with $(\eta + \theta)$, for $p = 1$, $\eta = 3$, $\theta = 1$, $\gamma = 1$ and $\delta = 2$, when $Z = 5$ is prime. But if such pairings occur simultaneously, so both η and θ are either odd or even, and likewise γ and δ , then Z is even $\neq 2$.

Let $j(\gamma - \delta) = k(\gamma + \delta)$ and choose arbitrarily $\gamma > \delta$. Then

$$Z = \frac{1}{2}((\gamma - \delta)/k)[\eta((j + k)X + 2kW) + \theta((j - k)X - 2kW)].$$

For Z to factorise in the way specified, we need to ensure the θ term cannot be negative, so that the term in [] is not 1 or 2. The θ term is

$$\begin{aligned} \theta((j - k)X - 2kW) &= \theta\{(j - k)[\sum(s=0, (p-1)/2)[((j+k)/(j-k))^{p-1-2s}]] \\ &\quad - (j+k)[\sum(s=0, (p-3)/2)[((j+k)/(j-k))^{p-2-2s}]]\}\delta^{p-1}. \end{aligned}$$

This equates to $\theta(j - k)(\delta^{p-1})$, so for $(\gamma - \delta)/k > 2$, Z is not prime.

If $j(\gamma - \delta) = k(\eta + \theta)$, then choosing j and k positive, i.e. $(\gamma - \delta)/k > 1$, we have

$$Z = (\gamma - \delta)[(j/k)\delta^p + \eta(X + 2W)],$$

so Z factorises.

With $j(\gamma - \delta) = kX$ under scrutiny, we obtain

$$Z = (\gamma - \delta)[\eta((j/k)\gamma + W) + \theta((j/k)\delta - W)].$$

Suppose the term in [] was 1, then we would have $(j/k)\delta < W$, so we would deduce

$$X\delta < (\gamma - \delta)W = X\delta - \delta^p,$$

which is impossible, hence Z is not prime.

If $j(\eta - \theta) = k(\gamma + \delta)$, then

$$Z = (\eta - \theta)[(j/k)\theta X + \gamma^p],$$

and Z factorises, because $(\eta - \theta)/k > 1$.

If $j(\eta - \theta) = k(\eta + \theta)$, then choosing arbitrarily $\eta > \theta$,

$$Z = \frac{1}{2}(\eta - \theta)[((j/k) + 1)\gamma^p + ((j/k) - 1)\delta^p]$$

so since $j/k > 1$ and in *this* instance we specify $(\eta - \theta)/k > 2$, Z again factorises.

For the case $j(\eta - \theta) = kX$, allocating $\eta > \theta$, the value of Z is

$$Z = (\eta - \theta)[(j/k)(\gamma + \delta)\theta + \gamma^p].$$

Since $(\eta - \theta)/k > 1$, Z factorises.

Suppose $jX = kY$. Then

$$Z = \frac{1}{2}X[\eta((\gamma + \delta) + (\gamma - \delta)(j/k)) + \theta((\gamma + \delta) - (\gamma - \delta)(j/k))].$$

We can choose arbitrarily $\gamma > \delta$. To ensure the term in [] is not 1 or 2, we need to evaluate the θ term. Now

$$j/k = 1 + \{2(\delta\gamma^p - \gamma\delta^p)/((\gamma - \delta)(\gamma^p - \delta^p))\},$$

so the θ term is the positive value

$$\theta((\gamma + \delta) - (\gamma - \delta)(j/k)) = 2\theta\delta^p(\gamma + \delta)/(\gamma^p - \delta^p).$$

If X/k is even, so are γ and δ . For X/k odd, the $k[]$ term is even. So Z is not prime.

Now consider $j(\gamma + \delta) = kY$, which gives

$$Z = (\gamma + \delta)[(\eta\gamma + \theta\delta)(j/k) - W].$$

So combining the facts

$$(\eta\gamma + \theta\delta) > \gamma + \delta$$

and

$$Y - W \geq Y - 2W = X,$$

we verify that the term in [] is positive and > 1 , implying that Z factorises.

Lastly, for $j(\eta + \theta) = kY$, we evaluate that

$$Z = (\eta + \theta)[\gamma Y - W(\gamma + \delta) + \theta(\gamma - \delta)(j/k)]$$

so that

$$Z = (\eta + \theta)[\gamma X + W(\gamma - \delta) + \theta(\gamma - \delta)(j/k)],$$

and choosing arbitrarily $\gamma > \delta$ gives Z is not prime. ■

The same theorem carries over for η and θ *integers*, with *two* prime factors instead of one, because the terms in [] can now be ± 1 or ± 2 . ■

No representations of primes are of the form

$$\gamma^p - \delta^p,$$

except for the possibilities $p = 1$, or $\delta = (\gamma - 1)$ and p prime.

Proof. If $\alpha - \beta = \gamma^{\uparrow(p^m)} - \delta^{\uparrow(p^m)}$ is prime, with $\alpha, \beta, \gamma, \delta, \varepsilon, \mu \in \mathbf{N}$ from now on, then the *second FSFT* gives $m = 1$ (otherwise (*) above factorises), and

$$\alpha - \beta = [\alpha^{1/p} - \beta^{1/p}]\{\Sigma(s = 0, p - 1)[\alpha^{s/p}][\beta^{(p-1-s)/p}]\}$$

is prime, the derivation of which implies α and β are powers of p , i.e.

$$\alpha = \gamma^p, \beta = \delta^p,$$

and either

$$\gamma - \delta = 1$$

or

$$\Sigma(s = 0, p - 1)[\gamma^s][\delta^{p-1-s}] = 1,$$

the latter corresponding to $p = 1$, so we choose the former.

If p is *not* prime, say $p = jq$, then because

$$\gamma = \alpha^{1/p} = \alpha^{1/qj} = (\alpha^{1/q})^{\uparrow(1/j)}$$

is a natural number, so is $\alpha^{1/q}$, and similarly for $\beta^{1/q}$. Then the prime $\alpha - \beta$ can be represented by the product

$$(***) \quad [\alpha^{1/q} - \beta^{1/q}] \{ \Sigma(s = 0, q - 1) [\alpha^{s/q}] [\beta^{(q-1-s)/q}] \}.$$

Now if $a > 1$ and $x > y$, we obtain the inequality

$$(x - y)^a = (x - y)^{a-1}(x - y) < x^{a-1}(x - y) < x^a - y^a.$$

Inserting $x = \alpha^{1/p}$, $y = \beta^{1/p}$ and $a = p/q$ has the consequence

$$1 = [\alpha^{1/p} - \beta^{1/p}] = [\alpha^{1/p} - \beta^{1/p}]^{\uparrow(p/q)} < [\alpha^{1/q} - \beta^{1/q}].$$

Thus in (***) the first and second terms $\neq 1$, and all terms involve sums of natural numbers – a contradiction. Hence p is prime. ■

Under the conditions of the previous theorem, p divides

$$\gamma^p - \delta^p - 1.$$

Proof. By Fermat's theorem, if p is any prime and γ and δ are integers, then p divides $(\gamma^p - \gamma)$ and $(\delta - \delta^p)$, so p divides $(\gamma^p - \delta^p - \gamma + \delta) = (\gamma^p - \delta^p - 1)$. ■

Let $p > 2$ be even, $\gamma > \delta \geq 1$ and $\gamma - \delta \neq 1$, then

$$\gamma^p - \delta^p$$

has at least three factors.

Proof. Consider $\gamma^{\uparrow p} - \delta^{\uparrow p}$. This may, for even p , be factorised as

$$(\gamma - \delta)(\gamma^{p-1} + \gamma^{p-2}\delta + \gamma^{p-3}\delta^2 + \dots + \delta^{p-1})$$

or as

$$(\gamma + \delta)(\gamma^{p-1} - \gamma^{p-2}\delta + \gamma^{p-3}\delta^2 - \dots - \delta^{p-1}).$$

Since $\gamma - \delta \neq \gamma + \delta$, if there are only two factors, which is the minimum if $\gamma - \delta \neq 1$, then

$$\gamma - \delta = (\gamma^{p-1} - \gamma^{p-2}\delta + \gamma^{p-3}\delta^2 - \dots - \delta^{p-1})$$

and

$$\gamma + \delta = (\gamma^{p-1} + \gamma^{p-2}\delta + \gamma^{p-3}\delta^2 + \dots + \delta^{p-1}),$$

so adding these gives successively

$$\gamma = \gamma^{p-1} + \gamma^{p-3}\delta^2 + \dots + \gamma\delta^{p-2}$$

and

$$\gamma \geq \gamma^{p-1} + \gamma^{p-3} + \dots + \gamma,$$

which is impossible. ■

We cannot dispense with the condition $\gamma - \delta \neq 1$, because if $\gamma = 2$, $\delta = 1$ and $p = 4$, then $\gamma^p - \delta^p = 15$. A more general theorem follows next.

Let $p = (2^{\uparrow k_0})\Pi(i = 1, n)(q_i^{\uparrow k_i})$, where the q_i are distinct odd primes, and $\gamma > \delta \geq 1$. Then $\gamma^p - \delta^p$ has at least $\Sigma(i = 0, n)k_i$ factors, and at least $1 + \Sigma(i = 0, n)k_i$ factors when $\gamma - \delta \neq 1$.

Proof. Let $q_0 = 2$. For the first pass through, consider all factors of $p = \prod(i = 0, n) (q_i \uparrow k_i)$ except for one unexponentiated factor q_r . This product is just $x_r = \prod(i = 0, n) \prod(j = 0, k_i - 1, \text{omit } r \text{ for one } i)(q_i)$. Then $p = (x_r)(q_r)$. By the equation at the end of section 2.2

$$\gamma^p - \delta^p = [(\gamma \uparrow x_r) - (\delta \uparrow x_r)][\Sigma(s = 0, q_r - 1)[\gamma \uparrow x_r s][\delta \uparrow x_r(q_r - 1 - s)]].$$

We now have at least two factors. We can then expand out $(\gamma \uparrow x_r) - (\delta \uparrow x_r)$ recursively, using the same formula, yielding at least one extra factor each time.

We continue iteratively, until we end up with $\gamma - \delta$, which can be a proper factor or the trivial factor 1, which we ignore. We have now $\Sigma(i = 0, n)k_i$ iterations, giving at least $\Sigma(i = 0, n)k_i$ factors if $\gamma - \delta = 1$ or at least $1 + \Sigma(i = 0, n)k_i$ factors otherwise. ■

Let $p = (2 \uparrow k_0)t$, where $t = \prod(i = 1, n)(q_i \uparrow k_i)$, the q_i are distinct odd primes, and arrange $\gamma > \delta \geq 1$. Then $\gamma \uparrow p + \delta \uparrow p$ has at least $1 + \Sigma(i = 1, n)k_i$ factors.

Proof. t is odd, and may be represented in a similar manner as before as $t = (y_r)(q_r)$. By another formula at the end of section 2.2

$$\varepsilon^t + \mu^t = [(\varepsilon \uparrow y_r) + (\mu \uparrow y_r)][\Sigma(s = 0, q_r - 1)[\varepsilon \uparrow y_r s][(-\mu) \uparrow y_r(q_r - 1 - s)]].$$

Put $\varepsilon = \gamma \uparrow (2 \uparrow k_0)$ and $\mu = \delta \uparrow (2 \uparrow k_0)$. The number of factors is obtained by recursion as previously, where, if prime, the final factor $\varepsilon + \mu$ will not add to the result. ■

*If $p \neq 1$, $\chi_1 = (\delta \uparrow p) + (\varepsilon \uparrow p)$ is prime
and $\chi_2 = (\varepsilon \uparrow p) - (\mu \uparrow p)$ is prime
then $\chi_1 - \chi_2$ is not prime unless $\chi_1 = 5$ and $\chi_2 = 3$.*

Proof. $\chi_1 - \chi_2 = (\delta \uparrow p) + (\mu \uparrow p)$ is even $\neq 2$ or $= 2$, otherwise $\chi_1 = 2$ or $\chi_2 = 2$. Now both $p = 2^t$ and p is prime, so $p = 2$. If $\chi_1 - \chi_2 = 2$, then $\delta = \mu = 1$, so $(\varepsilon - 1) = 1$, $\varepsilon = 2$ and $\chi_1 = 5$ and $\chi_2 = 3$. If $\chi_1 = 2$ then $\delta = \varepsilon = 1$ and $\chi_2 = 1 - \mu^2$, which is impossible. So $\chi_2 = 2 = (\varepsilon - \mu)(\varepsilon + \mu)$, and if $(\varepsilon - \mu) = 1$ then $2 = 2\mu + 1$, which is impossible. Hence $\chi_1 - \chi_2$ is not prime or $\chi_1 = 5$ and $\chi_2 = 3$. ■

*If $p \neq 1$, $\chi_3 = (\delta \uparrow p) + (\varepsilon \uparrow p)$ is prime
and $\chi_4 = (\varepsilon \uparrow p) + (\mu \uparrow p)$ is prime
then $\chi_3 - \chi_4$ is not prime unless $\chi_3 = 5$ and $\chi_4 = 2$.*

Proof. This results from the previous theorem. Alternatively, assume $\chi_3 - \chi_4$ is prime. We prove a partial contradiction. Then $\chi_3 - \chi_4 = (\delta \uparrow p) - (\mu \uparrow p)$, so both $p = 2^t$ and p is prime, so $p = 2$ and $(\delta - \mu) = 1$. Suppose $\chi_3 \neq 2$ and $\chi_4 \neq 2$, then for $\chi_3 - \chi_4$ to be prime it must $= 2$. Hence $2 = \delta^2 - (\delta - 1)^2 = 2\delta - 1$, which is impossible. Hence we have primes $\chi_3 = \delta^2 + \varepsilon^2 \neq 2$ and $\chi_4 = (\delta - 1)^2 + \varepsilon^2 = 2$, so $\varepsilon = 1$, $\delta = 2$ and $\chi_3 = 2^2 + 1 = 5$. ■

We note that *the binomial expansion of $\gamma^p - \delta^p$ for $\gamma = (\delta + 1)$ is*

$$\Sigma(r = 1, p)[p! / r!(p - r)!] \delta^{p-r}.$$

That p divides $(\delta + 1)^p - \delta^p - 1$ is easy to prove directly by a binomial expansion, the expression being

$$p\delta^{p-1} + [p(p-1)/2]\delta^{p-2} + \dots + p\delta,$$

so if p is prime the factorial denominators do not divide p . ■

We extend the above result. *For p prime, p divides*

$$(\delta + 1)^p - (\delta - x)^p - x - 1.$$

Proof. For two adjacent numbers, p divides

$$(\delta + 1)^p - \delta^p - 1 \quad \text{and} \quad \delta^p - (\delta - 1)^p - 1.$$

Hence p divides their sum. The result follows by induction. ■

Corollary. *If p is prime, then p divides*

$$y^p - (y - x)^p - w$$

if and only if

$$x \equiv w \pmod{p}.$$

Putting $y = x$, this gives Fermat's little theorem, $y^p - y \equiv 0 \pmod{p}$, from the binomial theorem. ■

With $z = y - x$, we find that *if $y \not\equiv z \pmod{p}$ then*

$$\sum_{r=1}^p [y^{p-r} z^{r-1}] \equiv 1 \pmod{p}. \quad \blacksquare$$

If $y^p - y$ is divisible by p , then so is

$$y^{n(p-1)+1} - y.$$

Proof. Since $y^{2p-1} - y^p = y^{p-1}(y^p - y)$ is divisible by p , the sum $(y^{2p-1} - y^p) + (y^p - y)$ is also, with the general result following by recursion. The proof extends to divisibility by any natural number m instead of a prime p . ■

Examples. Putting $p = 3$, we have for any odd natural number q

$$y^q - y \equiv 0 \pmod{6},$$

and putting $p = 5$, so $q = 4n + 1$, or $p = 7$, giving $q = 6n + 1$, etc. implies

$$y^q - y \equiv 0 \pmod{6p}. \quad \blacksquare$$

Expressions with Bernoulli numbers B^k inside quotation marks will be written as a sum of terms, each of which is a power of B times some number. The powers of B are then interpreted as Bernoulli numbers.

Thus Faulhaber's formula becomes

$$1^{k-1} + 2^{k-1} + \dots + m^{k-1} = [“(m + B)^k - B^k”]/k,$$

and summing the Fermat little theorem terms

$$(1^p - 1) + (2^p - 2) + \dots + (y^p - y)$$

entails *the following expression is divisible by p :*

$$\{ [“(y + B)^{p+1} - B^{p+1}”]/(p + 1) \} - \frac{1}{2}y(y + 1). \quad \blacksquare$$

If we carry out the derivation for Fermat's little theorem again, this time explicitly, we find the general identity for any not necessarily prime q

$$y^q - y = q \sum_{r=1}^{q-1} \left\{ \frac{(q-1)!}{r!(q-r)!} \right\} \\ \left[\frac{(y+B-1)^{q-r+1} - B^{q-r+1}}{(q-r+1)} \right]. \blacksquare$$

A related use of the binomial theorem is, for $n > 1$ and p prime $> n - 2$, the expression

$$y^p - (y-p)^p + \sum_{k=1}^{n-2} (-1)^k \left[\frac{p!}{k!(p-k)!} \right] p^k y^{p-k} \\ \equiv 0 \pmod{p^n}. \blacksquare$$

Let p be odd > 5 . The following expressions are divisible by p , also $p - 2$, if prime.

$$(\delta + 1)^p - \delta^p - 1 - p\delta \left[\delta^{p-2} + \left[\frac{(p-1)}{2} \right] \delta (\delta^{p-4} + 1) + 1 \right], \\ (\delta + 1)^p - (\delta - 1)^p - p\delta^2 [p - 1 + 2\delta^{p-3}] - 2$$

and

$$(\delta + 1)^p - 2\delta^p + (\delta - 1)^p - p\delta [(p-1)\delta^{p-3} + 2].$$

Proof. The first expression is derived from a binomial expansion of $(\delta + 1)^p$, with the first three and last three terms subtracted. Considering factorial denominators, it is divisible by p or $p - 2$ when either of these are prime, or both when both are prime.

The second and third expressions are obtained from the first under the transformation $\delta \rightarrow -\delta$, respectively adding or subtracting this result from the first. \blacksquare

Let n be even and p be odd, with $p > 2n + 1$. Then the following expressions are divisible by all primes between $(p - n)$ and p inclusive:

$$(\delta + 1)^p - \sum_{r=0}^n \left\{ \frac{p!}{r!(p-r)!} \right\} \delta^r (\delta^{p-2r} + 1), \\ (\delta + 1)^p - (\delta - 1)^p - 2 \left\{ \sum_{r=0}^{n/2} \left[\frac{p!}{(2r)!(p-2r)!} \right] \delta^{2r} \right. \\ \left. + \sum_{r=1}^{n/2} \left[\frac{p!}{(2r-1)!(p-2r+1)!} \right] \delta^{p-2r+1} \right\}$$

and

$$(\delta + 1)^p + (\delta - 1)^p - 2 \left\{ \sum_{r=0}^{n/2} \left[\frac{p!}{(2r)!(p-2r)!} \right] \delta^{p-2r} \right. \\ \left. + \sum_{r=1}^{n/2} \left[\frac{p!}{(2r-1)!(p-2r+1)!} \right] \delta^{2r-1} \right\}.$$

Proof. By the binomial theorem, the first expression is equal to

$$\sum_{s=n+1}^p \frac{(p+1)!}{s!(p-s)!} \delta^s (\delta^{p-2s} + 1).$$

To determine the summation range, there are $p + 1$ terms in the expansion of $(\delta + 1)^p$, and we are subtracting $2(n + 1)$ terms, so the number remaining is $p - 2n - 1$. The upper range in the summation is $(p - 2n - 1)/2 + n + 1 = (p + 1)/2$.

To show $p > 2n + 1$, for there to be no cancellations with primes, the lowest factor term of the largest $p!/(p - s)!$ is $(p - n)$, and if prime this must be greater than the concurrent greatest divisor term of $p!/(p - s)!$ by $s = n + 1$.

Thus no factorial denominators divide primes in the numerator between $(p - n)$ and p .

Under the transformation $\delta \rightarrow -\delta$, we obtain

$$-(\delta - 1)^p - \left\{ \sum_{r=0}^{n/2} \left[\frac{p!}{(2r)!(p-2r)!} \right] \delta^{2r} (1 - \delta^{p-4r}) \right. \\ \left. + \sum_{r=1}^{n/2} \left[\frac{p!}{(2r-1)!(p-2r+1)!} \right] \delta^{2r-1} (1 - \delta^{p-4r+2}) \right\}$$

is divisible by all primes between $(p - n)$ and p inclusive.

Hence by adding this expression with the corresponding expression for $+\delta$, or by subtracting it, we obtain the two subsequent divisibility results. \blacksquare

We investigate analogues of Fermat's little theorem for primes between $(p - n)$ and p .

Let n be even and p be odd, with $p > 2n + 1$. Then the following expressions are divisible by all primes between $(p - n)$ and p inclusive:

$$\begin{aligned}
& (\delta + 1)^p - (\delta - x)^p - x - 1 - \sum_{(r=1, n)} [p! / [r!(p-r)!]] \\
& \quad \{ [“(\delta + B)^{p-r+1} - (\delta - x - 1 + B)^{p-r+1}]” / (p-r+1)] \\
& \quad + [“(\delta + B)^{r+1} - (\delta - x - 1 + B)^{r+1}]” / (r+1) \}, \\
& (\delta + 1)^p - (\delta - 1)^p - (\delta - x)^p + (\delta + x)^p - 2x - 2 \\
& \quad - 2 \sum_{(r=1, n/2)} \{ [p! / [(2r!)(p-2r)!]] \\
& \quad [“(\delta + B)^{2r+1} - (\delta - x - 1 + B)^{2r+1}]” / (2r+1)] \\
& \quad + [1 / [(2r-1)!(p-2r+1)!]] \\
& \quad [“(\delta + B)^{p-2r+2} - (\delta - x - 1 + B)^{p-2r+2}]” / (p-2r+2) \} \}
\end{aligned}$$

and

$$\begin{aligned}
& (\delta + 1)^p + (\delta - 1)^p - (\delta - x)^p - (\delta + x)^p \\
& \quad - 2 \sum_{(r=1, n/2)} \{ [p! / [(2r!)(p-2r)!]] \\
& \quad [“(\delta + B)^{p-2r+1} - (\delta - x - 1 + B)^{p-2r+1}]” / (p-2r+1)] \\
& \quad + [1 / [(2r-1)!(p-2r+1)!]] \\
& \quad [“(\delta + B)^{2r} - (\delta - x - 1 + B)^{2r}]” / 2r \} \}.
\end{aligned}$$

Proof. We use Faulhaber's formula, noting

$$\sum_{(s=0, x)} (\delta - s)^q = \sum_{(s=0, \delta)} s^q - \sum_{(s=0, \delta - x - 1)} s^q. \blacksquare$$

Put $y = \delta + 1 = x + 1$. Then by direct transcription the following expressions are divisible by all primes between $(p - n)$ and p , for n even, p odd and $p > 2n + 1$:

$$\begin{aligned}
& y^p - y - \sum_{(r=1, n)} [p! / [r!(p-r)!]] \\
& \quad \{ [“(y + B - 1)^{p-r+1} - (B - 1)^{p-r+1}]” / (p-r+1)] \\
& \quad + [“(y + B - 1)^{r+1} - (B - 1)^{r+1}]” / (r+1) \}, \\
& y^p - (y - 2)^p + 2(y - 1)^p - 2y \\
& \quad - 2 \sum_{(r=1, n/2)} \{ [p! / [(2r!)(p-2r)!]] \\
& \quad [“(y + B - 1)^{2r+1} - (B - 1)^{2r+1}]” / (2r+1)] \\
& \quad + [1 / [(2r-1)!(p-2r+1)!]] \\
& \quad [“(y + B - 1)^{p-2r+2} - (B - 1)^{p-2r+2}]” / (p-2r+2) \} \}
\end{aligned}$$

and

$$\begin{aligned}
& y^p + (y - 2)^p - 2(y - 1)^p \\
& \quad - 2 \sum_{(r=1, n/2)} \{ [p! / [(2r!)(p-2r)!]] \\
& \quad [“(y + B - 1)^{p-2r+1} - (B - 1)^{p-2r+1}]” / (p-2r+1)] \\
& \quad + [1 / [(2r-1)!(p-2r+1)!]] \\
& \quad [“(y + B - 1)^{2r} - (B - 1)^{2r}]” / 2r \} \}. \blacksquare
\end{aligned}$$

We now consider polynomial forms. If

$$x_i \equiv y_i \pmod{n} \text{ and } r_i \equiv s_i \pmod{n}$$

then

$$\sum r_i [x_i \uparrow t_i] \equiv \sum s_i [y_i \uparrow t_i] \pmod{n}.$$

If n is prime and

$$t_i = K_i n + u_i,$$

then by Fermat's little theorem

$$\sum r_i [x_i \uparrow t_i] \equiv \sum s_i [y_i \uparrow (K_i + u_i)] \pmod{n}. \blacksquare$$

For $m, p > 0, n, q > 1 \in \mathbf{N}$, there is an isomorphism between additive $k \pmod{n}$ and, for fixed q , multiplicative $q \uparrow k$, so for $k = p^m$, by the second FSFT example of section 4 with $f = 1$, we obtain

$$q \uparrow (p^m) \equiv 1 \pmod{(q-1)}.$$

Consequently

$$q \uparrow (\sum (p_i \uparrow m_i)) \equiv 1 \pmod{(q-1)},$$

so for any $u_i > 0 \in \mathbf{N}$ we derive the implication

$$\begin{aligned} \sum (t=1, u_i)(p_i \uparrow m_i) &= u_i(p_i \uparrow m_i), \\ q \uparrow (\sum u_i(p_i \uparrow m_i)) &\equiv 1 \pmod{(q-1)}. \end{aligned}$$

By the FAFT, we also obtain the following results for p odd:

$$q \uparrow (p^m) \equiv -1 \pmod{(q+1)}$$

and

$$q \uparrow (\sum (i=1, j)(p_i \uparrow m_i)) \equiv (-1)^j \pmod{(q+1)},$$

which indicates a corresponding equation extending to p_i even (put $p_i = 1, u_i = v_i \uparrow m_i$)

$$q \uparrow (\sum u_i(p_i \uparrow m_i)) \equiv (-1)^{\uparrow (\sum u_i p_i)} \pmod{(q+1)}. \blacksquare$$

For p odd prime *quadratic reciprocity* theorems follow from Fermat's little theorem by considering $y(y^{(p-1)/2} - 1)(y^{(p-1)/2} + 1) \equiv y((y^2)^{(p-1)/2} - 1) \equiv 0 \pmod{p}$, so all squares $\neq 0 \pmod{p}$ belong to the $(y^{(p-1)/2} - 1)$ equivalence class [31].

Both $y^{(p-1)/2} \equiv 1$ and $y^{(p-1)/2} \equiv -1 \pmod{p}$ have $(p-1)/2$ root positions. For squares, we assert (the *occupancy theorem*, proved later) that these are all occupied by specific numbers, so there is an isomorphism between complex roots $y^{(p-1)/2} = 1$ at one extremity and non-empty equivalence classes of $y^2 \pmod{p}$ with $y^{(p-1)/2} \equiv 1 \pmod{p}$ at the other. ■

The little theorem is more generally written as $yu(y^{(p-1)/2} - u^{(p-1)/2})(y^{(p-1)/2} + u^{(p-1)/2})$, for which *the LCFT implies*

$$u(y^p) - y(u^p) = (y^2 - u^2)W = (y^2 - u^2)\Sigma(r=0, (p-3)/2)[y^{2r+1}u^{p-2r-2}] \equiv 0 \pmod{p},$$

so that W factorises. ■

For p odd prime, quadratic reciprocity theorems give a factorisation of the Fermat expression $y^{n(p-1)+1} - y$, by considering $y(y^{n(p-1)/2} - 1)(y^{n(p-1)/2} + 1)$. ■

Our alternative formulation of the expression is

$$yu\{[y^{n(p-1)/2}] - [u^{n(p-1)/2}]\}\{[y^{n(p-1)/2}] + [u^{n(p-1)/2}]\},$$

so this time *the LCFT implies*

$$\begin{aligned} u(y^{n(p-1)+1}) - y(u^{n(p-1)+1}) &= (y^2 - u^2)W \\ &= (y^2 - u^2)\Sigma(r=0, (n(p-1)/2) - 1)[y^{2r+1}u^{n(p-1)-2r-1}] \equiv 0 \pmod{p}, \end{aligned}$$

and W again factorises further. ■

Note also the variation that *for p prime and $j > 0$*

$$0 \pmod{p} \equiv [(y \uparrow p) - y] \uparrow [p \uparrow (j-1)],$$

and since intermediate terms in the binomial expansion are $\equiv 0 \pmod{p}$

$$\begin{aligned} 0 \pmod{p} &\equiv [y \uparrow (p \uparrow j)] + \{(-y) \uparrow [p \uparrow (j-1)]\} \\ &\equiv y\{y \uparrow [(p \uparrow j) - 1] + (-1) \uparrow j\}. \end{aligned}$$

We derive the result when p is an odd prime that if j is odd

$$0 \pmod{p} \equiv y^{\{y^{\{(p \uparrow j) - 1\}/2} - 1\}} \{y^{\{(p \uparrow j) - 1\}/2} + 1\},$$

and if j is even

$$-2y \pmod{p} \equiv \text{the same expression.}$$

If $y \not\equiv 0 \pmod{p}$ in the latter, $-2 \pmod{p}$ uniquely factorises as either

$$(-1)(2) \pmod{p}$$

so

$$0, 1, 3 \text{ or } -2 \pmod{p} \equiv y^{\{(p \uparrow j) - 1\}/2}$$

or as

$$(1)(-2) \pmod{p}$$

so

$$0, 2, -1 \text{ or } -3 \pmod{p} \equiv y^{\{(p \uparrow j) - 1\}/2}. \blacksquare$$

The above technique can be used in the context of solving an n th degree polynomial equation with Heegner integer coefficients and at least $(n - 4)$ such integer solutions.

We note that $y \equiv 0 \pmod{p}$ and $y \equiv 1 \pmod{p}$ are always present, the latter as a square \pmod{p} . The following theorem is useful in determining some further $\equiv \pm 1 \pmod{p}$ interrelationships between various $y^{(p-1)/2}$.

Let $0 < y < p$, with p odd (for example p prime) and $m \in \mathbf{N}$, then

$$y^{(p-1)/2} \equiv (-1)^{(p-1)/2} (mp - y)^{(p-1)/2} \pmod{p}.$$

Proof. Firstly, consider $(p - 1)/2$ even. Then a binomial expansion of the right hand side, leaving out terms in mp to a power, which are $\equiv 0 \pmod{p}$, indicates that $y^{(p-1)/2} \equiv (-y)^{(p-1)/2} \pmod{p}$.

If $(p - 1)/2$ is odd, then the binomial expansion gives $y^{(p-1)/2} \equiv -(-y)^{(p-1)/2} \pmod{p}$. \blacksquare

Our theorem has the following consequences.

Taking the typical example for the $p = 11$ table below, y^5 repeats mod 11 in three regions, **A**, **B** and **C**, the above equation representing symmetries in regions **B** and **C**.

Table: $p = 11$, $(p - 1)/2 = 5$.

$y \equiv \pmod{p}$	y^5	$y^5 \pmod{11}$	region
0	0	0	A
1	1	1	B $0 < n \leq (p - 1)/2$
2	32	-1	
3	243	1	
4	1024	1	
5	3125	1	
6	7776	-1	C $(p - 1)/2 < n < p$
7	16807	-1	
8	32768	-1	
9	59049	1	
10	100000	-1	
$11 \equiv 0 \pmod{11}$			repeats

For $(p - 1)/2$ *odd*, if $0 < n \leq (p - 1)/2$, i.e. region **B**, then there are k terms $\equiv 1 \pmod{p}$ and $(p - 1)/2 - k$ terms $\equiv -1 \pmod{p}$, so there must be in the $(p - 1)/2 < n < p$ region **C**, k terms $\equiv -1 \pmod{p}$ and $(p - 1)/2 - k$ terms $\equiv +1 \pmod{p}$, giving the complete set of $(p - 1)/2$ root positions for both $1 \pmod{p}$ and $-1 \pmod{p}$.

If $(p - 1)/2$ is *even*, with the k terms $\equiv 1 \pmod{p}$ for region **B** below, there are k terms $\equiv 1 \pmod{p}$ in region **C**, opposite in sign to the odd case. Thus there are $2k$ slots for $2k = (p - 1)/2$ quadratic residues of 1^2 to $4k^2$ in the combined **B** and **C** region, and these slots in **B** (and **C**) are completely occupied. So $k = (p - 1)/4$ in the **B** region, and similarly the residues $\equiv -1 \pmod{p}$ occupy k slots in this region, likewise in region **C**.

Table: $p = 17$, $(p - 1)/2 = 8$.

$y \equiv \pmod{p}$	y^8	$y^8 \pmod{17}$	region
0	0	0	A
1	1	1	B $0 < n \leq (p - 1)/2$
2	256	1	
3	6561	-1	
4	65536	1	
5	390625	-1	
6	1679616	-1	
7	5764801	-1	
8	16777216	1	
9	43046721	1	C $(p - 1)/2 < n < p$
10	100000000	-1	
11	214358881	-1	
12	429981696	-1	
13	815730721	1	
14	1475789056	-1	
15	2562890625	1	
16	4294967296	1	
$17 \equiv 0 \pmod{17}$			repeats

■

Note the generalised Fermat little theorem with $q = (p - 1)/2$ prime gives a formula for $y^{(p-1)/2} \pmod{p}$.

We now prove the *occupancy theorem*.

If $m \neq n \leq (p - 1)/2$, with p prime, then $m^2 \neq n^2 \pmod{p}$.

Proof. We will prove that $m^2 - n^2 \equiv 0 \pmod{p}$ leads to a contradiction, which would mean $(m - n)(m + n) = kp$ for some k .

Say $m > n$, then $n < (p - 1)/2$, so $m + n < p - 1 < p$ and likewise $(m - n) < p - 1$. But p , being prime, must be a factor of $(m - n)$, $(m + n)$ or both, and this is impossible. ■

Since 1 is a square, it follows from the above considerations that *when* $(p - 1)/2$ *is even*, $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$, *and when* $(p - 1)/2$ *is odd*, $(-1)^{(p-1)/2} \equiv -1 \pmod{p}$. ■

We have dealt with recurrence relations between numbers of the form $y^{(p-1)/2} \pmod{p}$. Another useful relation to determine the value of $y^{(p-1)/2} \pmod{p}$ is

$$(uv)^{(p-1)/2} \pmod{p} \equiv [u^{(p-1)/2} \pmod{p}][v^{(p-1)/2} \pmod{p}]. \quad \blacksquare$$

A basic question is then: when is a prime a square (mod p)?

If we look at the table for squares, say in the (mod 7) example that follows, there are p squares from 0 to $p^2 - 1 \pmod{p^2}$, being $0^2, 1^2, \dots, (p-1)^2$.

Table: $p = 7$, squares (underlined) to $p^2 = 49$. Region **E** columns = region **F** columns.

region D	<u>0</u>
region E	<u>1</u> 2 3 <u>4</u> 5 6 7 8 <u>9</u>
region F	10 11 12 13 14 15 <u>16</u> 17 18 19 20 21 22 23 24 <u>25</u> 26 27 28 29 30 31 32 33 34 35 <u>36</u> 37 38 39 40 41 42 43 44 45 46 47 48
next p^2	<u>49</u>

Since, by the binomial theorem for squares,

$$(p + n)^2 \equiv n^2 \pmod{p},$$

these p squares fill, in p iterations (mod p), all the squares that are possible (mod p^2).

Likewise, since

$$(p - n)^2 \equiv n^2 \pmod{p},$$

those squares which are non-zero (mod p^2), repeat in just two non-overlapping sets (mod p^2), regions **E** and **F**.

Although the non-constructive ‘pigeon hole principle’ can act as a barrier to understanding, we now apply this principle here.

We have previously proved that there are $(p-1)/2$ non-zero squares (mod p). The first overlapping set $\neq 0$, in region **E**, being the first $(p-1)/2$ squares (mod p^2), maps to precisely $(p-1)/2$ separate squares (mod p), because otherwise there would be less than $(p-1)/2$ of them. We are using here full occupancy of the square slots. ■

A ‘crossing out’ method can be used, analogous to the ‘sieve of Eratosthenes’ for primes, for determining whether a number is or is not a square (mod p). Set up a grid of width p and depth $> (p-1)^2/4p$ and $< [(p-1)^2/4p] + 1$ with the first column labelled 0. Determine the column for a number n given by $n \pmod{p}$. Put an X in column 0, an X in column 1 with no space between columns 0 and 1, an X in column 4 with two spaces between columns 1 and 4, and so on, increasing the number of spaces by two each time and continuing into other rows if necessary. If the column corresponding to n is reached, it is a square (mod p), otherwise it is not. ■

Quadratic reciprocity is often introduced through binary quadratic forms, discussed in a later work, where we will prove the following ‘supplementary’ law:

$$2^{(p-1)/2} \equiv 1 \pmod{p} \text{ if } p \equiv \pm 1 \pmod{8},$$

$$2^{(p-1)/2} \equiv -1 \pmod{p} \text{ if } p \equiv \pm 3 \pmod{8}$$

and quadratic reciprocity itself, which states, for p and q distinct odd primes [10]

$$[p^{(q-1)/2} \pmod{q}][q^{(p-1)/2} \pmod{p}] \equiv (-1)^{(p-1)(q-1)/4}.$$

If we recast this as

$$[p^{(q-1)/2} \pmod{q}] \equiv [(-1)^{(q-1)/2} q^{(p-1)/2} \pmod{p}],$$

the theorem is seen to be equivalent to the form in which Gauss put it

Let p and q be distinct odd primes. If $q \equiv 1 \pmod{4}$, i.e. $(q-1)/2$ is even, then p is a square \pmod{q} if and only if q is a square \pmod{p} . If $q \equiv 3 \pmod{4}$, i.e. $(q-1)/2$ is odd, then p is a square \pmod{q} if and only if $-q$ is a square \pmod{p} . ■

We note in the table below that if a prime $p \pmod{12} \equiv 1$ or $-1 \pmod{p}$ then $3^{(p-1)/2} \equiv 1 \pmod{p}$, and if $p \pmod{12} \equiv 5$ or $-5 \pmod{p}$ then $3^{(p-1)/2} \equiv -1 \pmod{p}$.

Table: p prime, $q = 3$.

$3^{(p-1)/2} \equiv \pm 1 \pmod{p}$	$p \pmod{12}$
$9 \equiv -1 \pmod{5}$	5
$27 \equiv -1 \pmod{7}$	-5
$243 \equiv 1 \pmod{11}$	-1
$729 \equiv 1 \pmod{13}$	1
$6561 \equiv -1 \pmod{17}$	5
$19683 \equiv -1 \pmod{19}$	-5
$177147 \equiv 1 \pmod{23}$	-1
$4782969 \equiv -1 \pmod{29}$	5
$14348907 \equiv -1 \pmod{31}$	-5

This is part of a more general result, supplementary to quadratic reciprocity, relating a prime $p \pmod{4q}$ to $q^{(p-1)/2} \pmod{p}$.

We can evaluate all $(p-1)/2$ non-zero squares \pmod{p} by the method already given.

Quadratic reciprocity then gives, for a given prime $q < p$ that is such a square, there is a bijection between $q^{(p-1)/2} \pmod{p}$ and $\pm p^{(q-1)/2} \pmod{q}$, the latter of which depends on \pmod{q} , and for which a square or non-square p depends on $q \pmod{4}$.

Thus, $q = 0$ maps to $p = 0 \pmod{4q}$. If the $\pmod{4q}$ region does not contain 0, non-zero squares determined by $q^{(p-1)/2} \equiv 1 \pmod{p}$ are equivalent to half of the $4q$ values of $p \neq 0 \pmod{4q}$, and non-squares map to the remaining $2q$ values $\pmod{4q}$. ■

For p prime, if $y^t \equiv 1 \pmod{p}$, then for any $s \in \mathbf{N}$, since $y^{s(p-1)} \equiv 1 \pmod{p}$, there exists an $r = 1/s \pmod{p}$ such that

$$y^{(p-1)r} \equiv 1 \pmod{p}.$$

If y is prime, r must divide $(p-1)$, so likewise if y is composite. ■

For $0 < n < p$, (for example with p prime), $m \in \mathbf{N}$ and r a divisor of $(p-1)$, then

$$y^{(p-1)r} \equiv (-1)^{(p-1)r} (mp - y)^{(p-1)r} \pmod{p}.$$

Proof. The result parallels the argument of the previous theorem where we had $r = 2$, by using $(p-1)/r$ instead of $(p-1)/2$. ■

We now ask: *when is a number an rth power (mod p), with r a divisor of (p - 1)?*

Table: p = 7 and r = 3, cubes (underlined) to p³ = 343.

region I	<u>0</u>
region J	1 2 3 4 5 6
	7 <u>8</u> 9 10 11 12 13
	14 15 16 17 18 19 20
	21 22 23 24 25 26 <u>27</u>
region K	...
	63 <u>64</u> 65 66 67 68 69
	...
	119 120 121 122 123 124 <u>125</u>
next p³	...
	210 211 212 213 214 215 <u>216</u>
next p³	<u>343</u>

There are p rth powers from 0 to p^r - 1 (mod p^{↑r}), being 0^r, 1^r, ... (p - 1)^r.

Once again, by the binomial theorem,

$$(p + n)^r \equiv n^r \pmod{p},$$

these p rth powers fill, in r iterations (mod p), all the rth powers that are possible (mod p^{↑r}).

For r *even*, where effectively we are dealing with a certain type of square,

$$(p - n)^r \equiv n^r \pmod{p},$$

so those rth powers which are non-zero (mod p^{↑r}) repeat in just two non-overlapping sets (mod p^{↑r}), regions **J** and **K**. But for r *odd*

$$(p - n)^r \equiv -n^r \pmod{p},$$

yields no new information this way, although we are able to assert that for (p - 1)/r = 2 as above, the (y^{(p-1)/2} ± 1) (mod p) equivalence classes for squares and non-squares are equivalently partitioned as (y^{r(p-1)/2r} ± 1) (mod p). Thus in this case y^r belongs to the ((y^r)^{(p-1)/2r} ± 1) (mod p) equivalence classes, i.e. y^r ≡ ±1 (mod p). For (p - 1)/r = k, the y^r belong to the (y^r)^k ≡ 1 (mod p) equivalence classes. ■

4. Differences and sums of powers.

Standard results in [3] for the case p = 2 are: *Except for positive integers of the form 4k + 2, every positive integer can be represented as the difference of two squares.*

Also: *Every odd prime is uniquely the difference of two squares.*

Putting p = 2 in the general binomial expansion, we infer *these primes are in one of the forms:*

$$4k + 1 = (2k + 1)^2 - (2k)^2$$

or

$$4k + 3 = (2k + 2)^2 - (2k + 1)^2. \blacksquare$$

Prime differences of odd prime p powers are unique for given p and of the form

Prime difference, p odd prime	Form
$(4r + 1)^p - (4r)^p$	$4s + 1$
$(4r + 2)^p - (4r + 1)^p$	$4s + 3$
$(4r + 3)^p - (4r + 2)^p$	$4s + 3$
$(4r + 4)^p - (4r + 3)^p$	$4s + 1$
$(4r + 1 + u)^p - (4r + u)^p$	$4s + u(3 - u) + 1$

Proof. $(2t + 1)^p - (2t)^p$ is of the form (*terms divisible by 4*) + $2pt + 1$.

We define two equivalence classes having remainders of 1 or 3 under division of the above by 4. For t even = $2r$, this maps to the equivalence class given by $4s + 1$. For t odd = $2r + 1$, it is of the form $4s + 3$.

$(2t + 2)^p - (2t + 1)^p$ is of the form (*terms divisible by 4*) + $2pt + 3$. For t even = $2r$, this is of the form $4s + 3$, and for t odd = $2r + 1$, its partition is $4s + 1$.

The expression for the form $4s + u(3 - u) + 1$ is adjusted to give the table entries above it for $u = 0, 1, 2$ and 3 . Since the substitution $u \rightarrow 4n + u$ for the prime expression leaves the form in the same equivalence class, the formula extends to arbitrary $u \in \mathbf{N}$. ■

Let p be an odd prime. Differences of prime powers (*these are non-prime differences if $x \neq 0$*) are of the form

Difference, p odd	Form
$(4r + 1)^p - (4r - x)^p$	$4s - [(x + 1)(x^2 + 5x - 3)/3]$
$(4r + 2)^p - (4r + 1 - x)^p$	$4s - [(x + 1)(x^2 + 2x - 9)/3]$
$(4r + 3)^p - (4r + 2 - x)^p$	$4s - [(x + 1)(x^2 - x - 9)/3]$
$(4r + 4)^p - (4r + 3 - x)^p$	$4s - [(x + 1)(x^2 - 4x - 3)/3]$
$(4r + 1 + u)^p - (4r + u - x)^p$	$4s + (x + 1)[(3 - u)(u - (x/2)) + (ux/2) - (x/3)(x + 1/2) + 1]$

Proof. By the first table, chaining together (adding) the adjacent sums $[(4r + 1 + u)^p - (4r + u)^p] + [(4r + u)^p - (4r + u - 1)^p]$ results, by additive epimorphism, in a form equal to the sum of the adjacent forms.

Adding together x adjacent sums gives a number $(4r + 1 + u)^p - (4r + u - x)^p$.

The form expression

$$4s + (x + 1)[(3 - u)(u - (x/2)) + (ux/2) - (x/3)(x + 1/2) + 1]$$

results from its composition with adjacent sums as

$$4s + (x + 1)u(3 - u) - (1 + 2 + \dots + x)(3 - 2u) - (1.1 + 2.2 + \dots + x.x) + (x + 1),$$

where $(1 + 2 + \dots + x)$ is the arithmetic sum $x(x + 1)/2$ and

$$1^2 + 2^2 + \dots + x^2 = x[x^2 + (3/2)x + 1/2]/3 = x(x + 1)(x + 1/2)/3.$$

Once again, the substitution $u \rightarrow 4n + u$ in the expression for the number leaves it in the same form equivalence class. ■

The formulae in the above two tables are unchanged when p is an *odd* number > 1 rather than a prime, though for non-prime p none of the differences of powers is prime.

The adjacent differences below for even $p > 0$ powers are of the form

Difference, p even	Form
$(4r + 1)^p - (4r)^p$	$4s + 1$
$(4r + 2)^p - (4r + 1)^p$	$4s + 3$
$(4r + 3)^p - (4r + 2)^p$	$4s + 1$
$(4r + 4)^p - (4r + 3)^p$	$4s + 3$
$(4r + 1 + u)^p - (4r + u)^p$	$4s + (2u/3)(2u - 5)(u - 2) + 1$

Proof. Differences $(2t + 1)^p - (2t)^p$, where p is even, are of the form
(terms divisible by 4) $+ 2pt + 1 = 4s + 1$,
whereas differences $(2t + 2)^p - (2t + 1)^p$ for even p , are of the form
(terms divisible by 4) $+ 2^p - 1 = 4s + 3$.

The expression for the form $4s + (2u/3)(2u - 5)(u - 2) + 1$ is adjusted to give the table entries above it for $u = 0, 1, 2$ and 3 . Once again, since the substitution $u \rightarrow 4n + u$ for the difference expression leaves the form in the same equivalence class, the formula extends to arbitrary $u \in \mathbf{N}$. ■

Let $p > 0$ be even. Differences of even powers are of the form

Difference, p even	Form
$(4r + 1)^p - (4r - x)^p$	$4s - [(x + 1)(x^3 + 7x^2 + 13x - 3)/3]$
$(4r + 2)^p - (4r + 1 - x)^p$	$4s - [(x + 1)(x^3 + 3x^2 - x - 9)/3]$
$(4r + 3)^p - (4r + 2 - x)^p$	$4s - [(x + 1)(x^3 - x^2 - 3x - 3)/3]$
$(4r + 4)^p - (4r + 3 - x)^p$	$4s - [(x + 1)(x^3 - 5x^2 + 7x - 9)/3]$
$(4r + 1 + u)^p - (4r + u - x)^p$	$4s + [(x + 1)/3][(2u - 5)(u - 2)(2u - x) - (4u - 9)ux + (2u - 3)x(2x + 1) - x^2(x + 1) + 3]$

Proof. The proof is similar to that for odd p .

The form expression

$$4s + [(x + 1)/3][(2u - 5)(u - 2)(2u - x) - (4u + 1)ux + (6u + 1)(x(2x + 1)/3) - x^2(x + 1) + 3]$$

results from chaining together $(x + 1)$ forms beginning with

$$4s + (2u/3)(2u - 5)(u - 2) + 1$$

and ending with

$$4s + (2(u - x)/3)(2u - 5 - 2x)(u - 2 - x) + 1.$$

We use the further relation

$$1^3 + 2^3 + \dots + x^3 = x^2(x+1)^2/4$$

to obtain the final result. ■

We now look at $(4r+1+u)^p + (4r+u)^p$, which is of the form

$$4s + (1+u)^p + u^p.$$

For p even, irrespective of whether u is even or odd, this is of the form

$$4s + (1+2v)^p \equiv 4s + 1. \blacksquare$$

Let $p > 0$ be even. Sums of p powers are of the form

Sum, p even	Form
$(4r+1)^p + (4r-x)^p$	$4s + 1 + [x(x^3 + 8x^2 + 20x + 10)/3]$
$(4r+2)^p + (4r+1-x)^p$	$4s + 1 + [x(x^3 + 4x^2 + 2x - 10)/3]$
$(4r+3)^p + (4r+2-x)^p$	$4s + 1 + [x(x^3 - 4x - 6)/3]$
$(4r+4)^p + (4r+3-x)^p$	$4s + 1 + [x(x^3 - 4x^2 + 2x - 2)/3]$
$(4r+1+u)^p + (4r+u-x)^p$	$4s + 1 - [x/3][(2u-7)(u-3)(2u-x-1) - (4u-13)(u-1)(x-1) + (2u-5)(x-1)(2x-1) - (x-1)^2x + 3]$

Proof.

$$(4r+1+u)^p + (4r+u-x)^p =$$

$$[(4r+1+u)^p + (4r+u)^p] - [(4r+u)^p - (4r+u-x)^p].$$

In consequence, the theorem is obtainable from the result for p even in the previous table, under the substitution for that table of $u \rightarrow (u-1)$ and $x \rightarrow (x-1)$. ■

Adjacent sums of odd $p > 1$ powers are of the form

Sum, p odd	Form
$(4r+1)^p + (4r)^p$	$4s + 1$
$(4r+2)^p + (4r+1)^p$	$4s + 1$
$(4r+3)^p + (4r+2)^p$	$4s + 3$
$(4r+4)^p + (4r+3)^p$	$4s + 3$
$(4r+1+u)^p + (4r+u)^p$	$4s - (u/3)(2u-7)(u-1) + 1$

Proof. For p odd $= 2q + 1 > 1$ the aforementioned equivalence class for

$$(4r+1+u)^p + (4r+u)^p,$$

being $4s + (1+u)^p + u^p$, if $u = 2v + 1$ is odd, is of the form

$$4s + (2q+1)2v + 1 \equiv 4s + 2v + 1.$$

If v is even, it is of the form $4s + 1$, and if v is odd it is of the form $4s + 3$.

If u is even $= 2w$ with w even, the form is $4s + 1$, and if w is odd, the form is $4s + 3$.

As before, the expression for the form $4s - (u/3)(2u-7)(u-1) + 1$ fits the table entries above it for $u = 0, 1, 2$ and 3 . ■

Let $p > 1$ be odd. Sums of p powers are of the form

Sum, p odd	Form
$(4r + 1)^p + (4r - x)^p$	$4s + 1 + (x/3)[(x^2 + 6x + 2)]$
$(4r + 2)^p + (4r + 1 - x)^p$	$4s + 1 + (x/3)[(x^2 + 3x - 7)]$
$(4r + 3)^p + (4r + 2 - x)^p$	$4s + 3 + (x/3)[(x^2 - 10)]$
$(4r + 4)^p + (4r + 3 - x)^p$	$4s + 3 + (x/3)[(x^2 - 3x - 7)]$
$(4r + 1 + u)^p + (4r + u - x)^p$	$4s - (u/3)(2u - 7)(u - 1) + 1$ $- [x/2][(4 - u)(2u - x - 1)$ $+ (u - 1)(x - 1) - [(x - 1)(2x - 1)/3] + 2]$

Proof. This results from chaining

$$[(4r + 1 + u)^p + (4r + u)^p] - [(4r + u)^p - (4r + u - x)^p]$$

from previous formulae. ■

The tables we have presented are periodic in the variable x , in the sense that x and the variable $x + k$ are in the same equivalence class for some k .

Let $k \in \mathbf{N}$. For $p > 0$ even, sums and differences are periodic with $x \equiv x + 2k$. For $p > 1$ odd, sums and differences are periodic with $x \equiv x + 4k$.

Proof. The periodicity follows directly from the tables of adjacent sums and differences, the n in $x \equiv x + nk$ for differences being the smallest number which brings the form back to $4s + 4$ in $(n - 1)$ successive adjacent additions of entries in the tables. For sums, we are adding together two tables, the periodicity being due to the subtracted differences. ■

We will see next that by putting $\eta = 1$ and $\theta = 0$, or $\eta = 0$ and $\theta = 1$, allows us to express $(4r + 1 + u)^p$ and $(4r + u - x)^p$ directly.

Let p be odd and η and θ complex numbers. Then there exist s, t such that

$$\begin{aligned} \eta(4r + 1 + u)^p + \theta(4r + u - x)^p = \\ \eta[2(t + s) - (1/3)[u^3 - 3u^2 - u - 3]] \\ + \theta[2(t - s) + (1/3)[x^3 - 3(u - 2)x^2 + (3u^2 - 12u + 2)x \\ - u^3 + 6u^2 - 8u]]. \end{aligned}$$

Proof. Add linear combinations of the odd p sum and difference tables for general x . ■

Let p be even and η and θ complex numbers. Then there exist s, t such that

$$\begin{aligned} \eta(4r + 1 + u)^p + \theta(4r + u - x)^p = \\ \eta[2(t + s) + (1/3)[2u^3 - 9u^2 + 10u + 3]] \\ + \theta[2(t - s) + (1/3)[x^4 - (4u - 8)x^3 + (6u^2 - 24u + 20)x^2 \\ - (4u^3 - 24u^2 + 40u - 10)x - (2u^3 - 9u^2 + 10u)]. \end{aligned}$$

Proof. Add linear combinations of even p sum and difference tables for general x . ■

If we consider $(4r + v)^p + (4r + v)^{p-1}$ and $(4r + v)^p - (4r + v)^{p-1}$ for both p even and p odd ($p > 1$ and $r > 0$), we obtain the following table.

p	Formula	v	Form
odd	$(4r + v)^p + (4r + v)^{p-1}$	0	4s
		1	4s + 2
		2	4s
		3	4s
		v	4s + v(v - 3)(v - 2)
	$(4r + v)^p - (4r + v)^{p-1}$	0	4s
		1	4s
		2	4s
		3	4s + 2
		v	4s + (v/3)(v - 2)(v - 1)
even	$(4r + v)^p + (4r + v)^{p-1}$	0	4s
		1	4s + 2
		2	4s + 2
		3	4s
		v	4s - v(v - 3)
	$(4r + v)^p - (4r + v)^{p-1}$	0	4s
		1	4s
		2	4s + 2
		3	4s + 2
		v	4s - (v/3)(2v - 7)(v - 1)

■

Suppose, as an example, we wanted to obtain, mod 4, the value of

$$(4r + v)^p + (4r + v)^{p-y}$$

for p odd and y even. The mod 4 form consists of one term for p odd:

$$[(4r + v)^p + (4r + v)^{p-1}],$$

with (y/2) terms considered for (p - 1) even (the example uses y = 4):

$$- [(4r + v)^{p-1} - (4r + v)^{p-2}] - [(4r + v)^{p-3} - (4r + v)^{p-4}],$$

and (y - 2)/2 terms, considered for (p - 2) odd:

$$- [(4r + v)^{p-2} - (4r + v)^{p-3}].$$

By this and similar techniques we obtain

p	Formula	y	Form
odd	$(4r + v)^p + (4r + v)^{p-y}$	odd	4s + [v(v - 3)/2][y(v - 1) + (v - 3)]
		even	4s + [2v/3](2v - 5)(v - 2) + [yv/6](v - 5)(v - 1)
	$(4r + v)^p - (4r + v)^{p-y}$	odd	4s - [v(v - 1)/6][y(v - 5) - 3(v - 3)]
		even	4s + [yv/2](v - 3)(v - 1)
even	$(4r + v)^p + (4r + v)^{p-y}$	odd	4s + [v(v - 3)/2][-y(v - 1) - (v - 3)]
		even	4s - [2v/3](v ² - 3v - 1) + [yv/6](v - 5)(v - 1)
	$(4r + v)^p - (4r + v)^{p-y}$	odd	4s - [v(v - 1)/6][y(v - 5) + 3(v - 3)]
		even	4s - [yv/2](v - 3)(v - 1)

To check, we may have to use

$$(v/3)(v - 5)(v - 1) = v(v - 3)(v - 1) \pmod{4},$$

since there may be more than one way to obtain these formulae. ■

Of special note is that, by subtracting terms like $(4r + v)^p - (4r + v)^{p-1}$, for p even we can now obtain terms elliptic in u and x from the previously derived sums and differences of powers for p odd.

Formula, p even, $r > 0$	Form
$(4r + 1 + u)^p - (4r + u - x)^p$	$4s - (2x^3/3) - 3x^2 - (4x/3) + 1 + 2u(-u + 2 + x^2 + 3x - ux)$
$(4r + 1 + u)^p + (4r + u - x)^p$	$4s + (2x^3/3) + 3x^2 + (4x/3) + 1 + 2u(-x + u - 3)$

■

Using a typical formula such as

$$(4r + 1 + u)^{p-y} - (4r + u - x)^p = (4r + 1 + u)^p - (4r + u - x)^p - [(4r + 1 + u)^p - (4r + 1 + u)^{p-y}]$$

and putting $v = (1 + u)$ or $v = (u - x)$, the sum and difference tables of section 5 for p odd, and the above table for p even, then give formulae (mod 4) for arbitrary sums and differences of powers. Thus for both p even and p odd we obtain the following elliptic curves in u and x , linear in y , reduced mod 4.

p	Formula	y	Form
odd	$(4r + 1 + u)^p + (4r + u - x)^{p-y}$	odd	$4s - (u/3)(2u - 7)(u - 1) + 1 - (x/2)[(4 - u)(2u - x - 1) + (u - 1)(x - 1) - [(x - 1)(2x - 1)/3] + 2] + [(u - x)(u - x - 1)/6][y(u - x - 5) - 3(u - x - 3)]$
		even	$4s - (u/3)(2u - 7)(u - 1) + 1 - (x/2)[(4 - u)(2u - x - 1) + (u - 1)(x - 1) - [(x - 1)(2x - 1)/3] + 2] - [y(u - x)/2](u - x - 3)(u - x - 1)$
	$(4r + 1 + u)^{p-y} + (4r + u - x)^p$	odd	$4s - (u/3)(2u - 7)(u - 1) + 1 - (x/2)[(4 - u)(2u - x - 1) + (u - 1)(x - 1) - [(x - 1)(2x - 1)/3] + 2] + [(u + 1)u/6][y(u - 4) - 3(u - 2)]$
		even	$4s - (u/3)(2u - 7)(u - 1) + 1 - (x/2)[(4 - u)(2u - x - 1) + (u - 1)(x - 1) - [(x - 1)(2x - 1)/3] + 2] - [y(u + 1)/2](u - 2)u$
	$(4r + 1 + u)^p - (4r + u - x)^{p-y}$	odd	$4s + (x + 1)[(3 - u)(u - (x/2)) + (ux/2) - (x/3)(x + 1/2) + 1] - [(u - x)(u - x - 1)/6][y(u - x - 5) - 3(u - x - 3)]$
		even	$4s + (x + 1)[(3 - u)(u - (x/2)) + (ux/2) - (x/3)(x + 1/2) + 1] + [y(u - x)/2](u - x - 3)(u - x - 1)$
	$(4r + 1 + u)^{p-y} - (4r + u - x)^p$	odd	$4s + (x + 1)[(3 - u)(u - (x/2)) + (ux/2) - (x/3)(x + 1/2) + 1] + [(u + 1)u/6][y(u - 4) - 3(u - 2)]$
		even	$4s + (x + 1)[(3 - u)(u - (x/2)) + (ux/2) - (x/3)(x + 1/2) + 1] - [y(u + 1)/2](u - 2)u$
even $r > 0$	$(4r + 1 + u)^p + (4r + u - x)^{p-y}$	odd	$4s + (2x^3/3) + 3x^2 + (4x/3) + 1 + 2u(-u + 2 + x^2 + 3x - ux) + [(u - x)(u - x - 1)/6][y(u - x - 5) - 3(u - x - 3)]$

		even	$4s + (2x^3/3) + 3x^2 + (4x/3) + 1 + 2u(-u + 2 + x^2 + 3x - ux) + [y(u - x)/2](u - x - 3)(u - x - 1)]$
$(4r + 1 + u)^{p-y} + (4r + u - x)^p$		odd	$4s + (2x^3/3) + 3x^2 + (4x/3) + 1 + 2u(-u + 2 + x^2 + 3x - ux) + [(u + 1)u/6][y(u - 4) + 3(u - 2)]$
		even	$4s + (2x^3/3) + 3x^2 + (4x/3) + 1 + 2u(-u + 2 + x^2 + 3x - ux) + [y(u + 1)/2](u - 2)u$
$(4r + 1 + u)^p - (4r + u - x)^{p-y}$		odd	$4s - (2x^3/3) - 3x^2 - (4x/3) + 1 + 2u(-u + 2 + x^2 + 3x - ux) + [(u - x)(u - x - 1)/6][y(u - x - 5) + 3(u - x - 3)]$
		even	$4s - (2x^3/3) - 3x^2 - (4x/3) + 1 + 2u(-u + 2 + x^2 + 3x - ux) - [y(u + 1)/2](u - 2)u$
$(4r + 1 + u)^{p-y} - (4r + u - x)^p$		odd	$4s - (2x^3/3) - 3x^2 - (4x/3) + 1 + 2u(-u + 2 + x^2 + 3x - ux) + [(u + 1)u/6][y(u - 4) + 3(u - 2)]$
		even	$4s - (2x^3/3) - 3x^2 - (4x/3) + 1 + 2u(-u + 2 + x^2 + 3x - ux) + [y(u + 1)/2](u - 2)u$

The corresponding formulae for e.g.

$$\eta(4r + 1 + u)^p + \theta(4r + u - x)^{p-y}$$

can be obtained from the above sums and differences.

The above formulae have a finite number of integer solutions mod 4, arising from the periodicity in u , x and y – a maximum of $2^8 = 256$ possibilities, given that p has two sets of solutions, for even and odd, and the first exponent is or is not less than the second. Explicit calculations reduce this – less than the number of solutions derived in elliptic curve theory from a direct application of Siegel’s theorem [26], [27]. The theorem of Mazur puts limits on the torsion subgroup, giving crudely less than 240 possibilities [20], [21]. ■

Rather than use reduction mod 4, we can proceed as follows.

$$(q + v)^p - (q + v)^{p-1} = qs + v^{p-1}(v - 1),$$

thus by ‘chaining’

$$(q + v)^p - (q + v)^{p-y-1} = qs + v^{p-y-1}(v^{y+1} - 1). \blacksquare$$

Exercise. René Schoof [25] poses the problem – for exponents ≥ 2 , when are differences of powers of the form $2 \pmod{4}$? We ask, does 2 only $= 3^3 - 5^2$ in powers?

We will write such differences in the form $(A + B)$ where

$$A = m^p - n^p$$

and

$$B = n^p - n^{p-y},$$

or of the form $(C + A)$, where

$$C = m^{p-y} - m^p.$$

Since B and C are always even, so is A .

We first investigate the cases for A – where A is even.

A factorises as

$$(m - n)(m^{p-1} + m^{p-2}n + \dots + n^{p-1}).$$

Because A is not odd, so $n \neq m - 1$, the factorisation exists.

If m and n are even, then $A \equiv 0 \pmod{4}$.

Otherwise, m and n are odd.

If p is even, then

$$\begin{aligned} A &= (m - n)(\text{an even number of terms, each of which is odd}) \\ &\equiv 0 \pmod{4}. \end{aligned}$$

If p is odd, if both m and n are of the form $4r + 1$, or both are of the form $4r + 3$, then $m - n = 4r$, so

$$A \equiv 0 \pmod{4}.$$

If p is odd, if m is of the form $4r + 1$ and n is of the form $4r + 3$, or vice-versa, then since we are dealing with

$$A = (m - n)(\text{an odd number of terms, each of which is odd}),$$

then

$$A \equiv 2 \pmod{4}.$$

This exhausts all the cases for the structure of $A = m^p - n^p$, for A even.

We investigate

$$B = n^p - n^{p-y}.$$

Write

$$n = 4r + j.$$

Then

$$B = (4r + j)^{p-y}((4r + j)^y - 1).$$

If $n = 4r + 1$, then

$$B \equiv (4r + 1)(4r + 1 - 1) \equiv 4r \equiv 0 \pmod{4},$$

so for $n = 4r + 1$ there is only one case, irrespective of whether y is even or odd.

If $n = 4r + 3$, and y is even, then

$$(4r + 3)^y \equiv 1 \pmod{4}, \text{ so } B \equiv 4r \equiv 0 \pmod{4}.$$

If $n = 4r + 3$, and y is odd, then

$$B = (4r + 3)^{p-y}(4r + 2) \equiv 4r + 2 \equiv 2 \pmod{4}.$$

If n is even, if $n = 4r$ then $B \equiv 0 \pmod{4}$. If $n = 4r + 2$, if $p - y = 1$ then

$$B \equiv (4r + 2)(4r + 3) \equiv 2 \pmod{4},$$

and if $p - y = 1$, y is even and p is odd for $n = 4r + 2$, then

$$B \equiv (4r + 2)(4r + 1) \equiv 2 \pmod{4},$$

otherwise if $p - y \neq 1$, then

$$B \equiv 0 \pmod{4}.$$

We note that if n is negative, then if the case n positive is of the form $4r + 1$, then $-n$ is of the form $4r + 3$, likewise $n = 4r + 3$ implies $-n = 4r + 1$. This is a salient feature of our calculations, since if $p - y$ is even, we may need to include the case $(-n)^{p-y} = n^{p-y}$.

This exhausts all the cases covering B .

We now work out explicitly configurations for C, which is negative for $y > 0$. The argument parallels that for B exactly. We write

$$m = 4r + k,$$

so that

$$C = (4r + k)^{p-y}(1 - (4r + k)^y).$$

Allocating $m = 4r + 1$ gives

$$C \equiv (4r + 1)(1 - 4r - 1) \equiv -4r \equiv 0 \pmod{4},$$

whereas if $m = 4r + 3$, first considering y even,

$$(4r + 3)^y \equiv 1 \pmod{4},$$

so in this case

$$C \equiv (4r + 1)(1 - 4r - 1) \text{ or } (4r + 3)(1 - 4r - 1) \equiv 0 \pmod{4},$$

and for the y odd case

$$C \equiv (4r + 1)(1 - 4r - 3) \text{ or } (4r + 3)(1 - 4r - 3) \equiv 2 \pmod{4}.$$

The case for m even is likewise similar, which gives $C \equiv 0 \pmod{4}$ if $p - y \neq 1$.

The comment for B on $(-n)^{p-y}$ solutions also holds for C with $(-m)^{p-y}$ solutions. This is apposite, since a reversal of sign for m in both A and C results in a cancellation of both $(-m)^p$ terms in $(C + A)$.

If $(A + B)$ or $(C + A) \equiv 2 \pmod{4}$, then for $(A + B)$, $A \equiv 0 \pmod{4}$ and $B \equiv 2 \pmod{4}$, or vice-versa, and similarly for $(C + A)$.

For $(A + B)$, if $A \equiv 0 \pmod{4}$, then m and n are even, so $n = 4r + 2$, y is odd and p is even or y is even and p is odd, and $p - y = 1$, which breaks the stipulation of the problem that $p - y \neq 1$, so there are no such cases.

If $A \equiv 2 \pmod{4}$, then p is odd, m is of the form $4r + 1$, n is like $4r + 3$ or vice-versa, and $B \equiv 0 \pmod{4}$, so if $n = 4r + 1$ this satisfies, but if $n = 4r + 3$, then y is even.

Thus, if we consider A with $B \equiv 0 \pmod{4}$, then the lowest such positive numbers A are for p odd > 1 , with $m = 4r + 1$ and $n = 4r + 3$ or vice-versa,
 $3^3 - 1^3 = 26$, $5^3 - 3^3 = 98$, $7^3 - 5^3 = 218$, $3^5 - 1^5 = 242$, $7^3 - 1^3 = 342$, etc.

For the same $A \equiv 2 \pmod{4}$ with $|m| > |n|$, where $|m|$ is the positive magnitude $\sqrt{(m^2)}$, we generate additional $(A + B)$ entries for $n = 4r + 1$ with freedom for y (which can also be negative), i.e. the additional terms for low powers

$$7^3 - (-3)^4 = 262, 7^3 - 5^2 = 318, 7^3 - (-3)^2 = 334$$

and if $|m| \leq |n|$ we obtain, for low values of m and n , the $(A + B)$ terms

$$3^3 - 5^2 = 2, 3^3 - (-3)^2 = 18, 3^5 - 5^3 = 118, 3^5 - 5^2 = 218, 3^5 - (-3)^2 = 234, \text{ etc.}$$

For $n = 4r + 3$ and $|m| > |n|$, we have the extra lowest term $5^5 - 3^3 = 3098$.

We now realise that all terms with the $(A + B)$ structure: positive $m >$ positive n and $y \geq 0$ are ≥ 26 , the lower powers and values of m and n generating the lowest $(A + B)$.

If $A \equiv 0 \pmod{4}$ for $(A + C)$, then $m = 4r + 2$. In the case $C \equiv 2 \pmod{4}$, $p - y = 1$ again – which does not satisfy the problem criteria.

Accordingly, $A \equiv 2 \pmod{4}$ and $C \equiv 0 \pmod{4}$. For $|m| > |n|$ and $b = 4r + 1$, y is even, so we can consider a low value of $(C + A)$ corresponding to a relatively high value of m , e.g.

$$15^3 - 5^5 = 250.$$

In this and the next case, if $|m| < |n|$ and $y > 0$, all $(C + A)$ terms are negative.

For $(C + A)$, if $n = 4r + 3$, so $m = 4r + 1$, $p - y$ is free to range above 1. If $|m| > |n|$ then we have low terms like

$$(-7)^2 - 3^3 = 22, 5^4 - 3^5 = 382, 9^3 - 3^5 = 486, (-7)^4 - 3^5 = 2158, \text{ etc.}$$

Some of these terms can be quite small, e.g.

$$13^3 - 3^7 = 10. \blacksquare$$

References.

1. J.H. Adams, *Exponentiation* [this work], <http://www.jimhadams.com/math/ExponentialFactorisationTheorems.pdf>, (October 5 2009).
2. Z.I. Borevich and I.R. Shafarevich, *Number Theory*, Academic Press, (1966).
3. D.M. Burton, *Elementary Number Theory*, Wm.C. Brown, (1989).
4. J.H. Conway and R.K. Guy, *The Book of Numbers*, Copernicus Books, (2006).
5. J.H. Conway and D.A. Smith, *On Quaternions and Octonions*, A.K. Peters, (2003).
6. G. Cornell, J.H. Silverman and G. Stevens eds, *Modular Forms and Fermat's Last Theorem*, Springer-Verlag, (1997).
7. J. Daems, *A Cyclotomic Proof of Catalan's Conjecture*, <http://www.math.leidenuniv.nl/~jdaems/scriptie/Catalan.pdf>, (September 29 2003).
8. P.G.L. Dirichlet, *Mémoire sur l'impossibilité de quelques équations indéterminées du cinquième degré*, *Mathematische Werke*, vol. 1, 21-46.
9. Ebbinghaus et al., *Numbers*, Springer (1991).
10. H.M. Edwards, *Fermat's Last Theorem*, Springer (1977).
11. R.K. Guy, *Unsolved Problems in Number Theory*, Springer (2004).
12. W.R. Hamilton, *Elements of Quaternions*, Vol I, page 275, reprint Chelsea, (1969).
13. H. Jacquet and R.P. Langlands, *Automorphic Forms on $GL(2)$* , Springer-Verlag, (1970).
14. E.E. Kummer, *Collected Papers*, ed. André Weil, vol. 1, *Contributions to Number Theory*, Springer-Verlag, (1975).
15. E.E. Kummer, *De numeris complexis, qui radicibus unitatis et numeris integris redibus constant*, *ibid.* 165-192.
16. E.E. Kummer, *Beweis des Fermat'schen Satzes der Unmöglichkeit von $x^\lambda + y^\lambda = z^\lambda$, für eine unendliche Anzahl Primzahlen λ* , *ibid.* 274-297.
17. F.W. Lawvere and R. Rosebrugh, *Sets for Mathematics*, Cambridge University Press, (2003).
18. S. Mac Lane, *Categories for the Working Mathematician*, Second Edition, Springer (1997).
19. Yu.I. Manin and A.A. Panchiskin, *Introduction to Modern Number Theory*, Springer, (2005, 2007).
20. B. Mazur, *Modular Curves and the Eisenstein Ideal*, *IHES Publ. Math* **47**, 33-186, (1977).
21. B. Mazur, *Rational Isogenies of Prime Degree*, *Invent. Math.* **44**, 129-162, (1978).
22. T. Metsänkylä, *Catalan's Conjecture: Another Old Diophantine Problem Solved*, *Bull. Amer. Math Soc.* **41**, 43-57, (2003).
23. P. Mihăilescu, *Primary Cyclotomic Units and a Proof of Catalan's Conjecture*, *J. reine angew. Math* **572**, 167-195, (2004).

24. J. Rotman, *Galois Theory*, Second Edition, Springer (1998).
25. R. Schoof, *Catalan's Conjecture*, Springer-Verlag, (2008).
26. J.H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, (1992).
27. J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, (1986).
28. R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. Math., II. Ser. 141, No. 3, 553-572, (1995).
29. A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. Math., II. Ser. 141, No. 3, 443-551, (1995).
30. L.C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, (1982).
31. H. Weyl, *Algebraic Theory of Numbers*, Princeton University Press, (1940).

JIM ADAMS